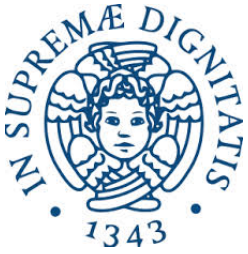


UNIVERSITÀ DI PISA

Dipartimento di Matematica

Dottorato di Ricerca in Matematica

Tesi di Dottorato

EXTENSIONS OF p-POWER DEGREE OF A p-ADIC FIELD

Maria Rosaria Pati

Relatore: Prof. Roberto Dvornicich

23 Settembre 2016

To everyone
who believes in me.

Contents

Contents i

Introduction ii

1 Preliminaries 1

1.1 Basic properties of extensions of local fields 1

1.2 Basics on linear representation theory 6

1.3 The correspondence theorem 8

2 Extensions of degree p^ℓ 15

2.1 Improving the correspondence theorem for p^ℓ extensions 15

2.2 The total number of isomorphism classes 19

2.3 Classifying according to the Galois group 21

2.4 Ramification groups and Discriminant 27

2.5 The field F when $\ell = 2$ 33

3 Extensions of degree p^4 36

3.1 Number of classes and Galois groups when $4 \mid f_K$ 37

3.2 Number of classes and Galois groups when $4 \nmid f_K$ 39

Bibliography 56

Introduction

The goal of this thesis is to classify a certain kind of extensions of degree a power of p of a p-adic field. It is well known that a p-adic field K has only a finite number of non-isomorphic algebraic extensions with given degree [Kra66]. Among these, the unramified and tamely ramified extensions are well-known being generated by a specific type of polynomials, while the wildly ramified ones are still a bit mysterious and so become the object of our study. This means that we concentrate on totally ramified extensions of K of degree p^k where k is any natural number, in particular we try to count their number up to K-isomorphism and to classify them according to the Galois group of their normal closure, although only in the simplified case of extensions having no intermediate fields.
In 2007 Dvornicich and Del Corso [DCD07], looking at the isomorphism classes of extensions of K of degree p, gave a new way to attack the problem of counting extensions: their idea is to "shift" the p-extensions of K in a more easy environment, where they can be identified by the action of a certain group on a suitable space.
Recently in [DCDM], Del Corso, Dvornicich and Monge, taking inspiration from [DCD07], present a general and very useful way to study the extensions of degree p^k of a p-adic field having no intermediate extensions. Denoting by F the composite of all normal and tame extensions of K whose Galois group is a subgroup of $\mathrm{GL}(k, \mathbb{F}_p)$ and by H the group $\mathrm{Gal}(F/K)$, they show that (see Theorem 1.8)

Theorem 0.1. *There exists a natural one-to-one correspondence between the isomorphism classes of extensions of K of degree p^k ($k \geq 1$) having no intermediate extension and the irreducible H-submodules of F^*/F^{*p} of dimension k of the Galois module F^*/F^{*p}. The isomorphism class $[L/K]$ corresponds to Ξ where $LF = F(\sqrt[p]{\Xi})$, and $\mathrm{Gal}(LF/K)$ is always a split extension of $\mathrm{Gal}(F/K)$.*

This key result allows one to classify the extensions of K of p-power degree only

by studying the structure of the filtered $\mathbb{F}_p[H]$-module F^*/F^{*p}; in other words, our problem is reduced to find the irreducible representations of dimension k of a certain group H acting on the suitable module F^*/F^{*p}.

The study of the structure of F^*/F^{*p} as $\mathbb{F}_p[H]$-module is the task of Chapter 1 of this thesis, which, after a brief recall of the objects and the basic facts we deal with, gives a detailed description of the $\mathbb{F}_p[H]$-submodules of F^*/F^{*p}. This description (in some measure) does not depend on the field F defined above and it holds for a large class of extensions of K, provided that it is tamely ramified over K. In particular, it holds for the field F defined in Chapter 2, which is the smallest field we can take working in the correspondence theorem when k is equal to a fixed prime number ℓ.

Unfortunately the trick of looking at certain representations to study wild extensions is not usable in the general case of extensions of degree p^k, with k any natural number. As outlined before, we have successfully used it to count the isomorphism classes of the extensions of degree p^ℓ where ℓ is a prime number (see Chapter 2), and in Chapter 3 we apply the same method to study the first non prime case, $k = 4$. This latter case shows how laborious the study becomes when the number of divisors of k increases, in fact such increase causes an explosion of the number of representations of H in F^*/F^{*p} and as a consequence of the number of cases to deal with.

When it is applicable, Theorem 0.1 allows not only to count the number of isomorphism classes, but also to determine the Galois group of their normal closure and to count how many of them contain extensions whose normal closure has a prescribed Galois group, for each of the possible groups that can appear as Galois group. In fact, if L/K is an extension of degree admissible to apply Theorem 0.1 and $\tilde{L}$ is its normal closure then

$$\mathrm{Gal}(\tilde{L}/K) \simeq V \rtimes_{\bar{\rho}} \bar{H}$$

where $\bar{\rho}$ is the map induced on the quotient $\bar{H} = H/\ker\rho$ and the pair (V, ρ) is the representation of H in F^*/F^{*p}, which corresponds to the class of L/K under the correspondence of Theorem 0.1. In other words, $\mathrm{Gal}(\tilde{L}/K)$ is the semidirect product of V with the largest quotient of H acting faithfully on it. Fixing a basis of the $\mathbb{F}_p$-vector space V, we can identify the image of ρ with a subgroup of $\mathrm{GL}(\mathbb{F}_p)$, so that if $[L : K] = p^k$ then $\mathrm{Gal}(\tilde{L}/K) \simeq (\mathbb{F}_p)^k \rtimes \mathcal{H}_\rho$ where $\mathcal{H}_\rho$ represents the action of $\bar{H}$ on V given by $\bar{\rho}$, expressed with respect to the fixed basis. Moreover the normal

closures of two isomorphism classes have the same Galois group if and only if

$$(\mathbb{F}_p)^k \rtimes \mathcal{H}_\rho \simeq (\mathbb{F}_p)^k \rtimes \mathcal{H}_{\rho'}$$

and this happens if and only if the two subgroups $\mathcal{H}_\rho$, $\mathcal{H}_{\rho'}$ of $\mathrm{GL}(k, \mathbb{F}_p)$ are conjugate over $\mathrm{GL}(k, \mathbb{F}_p)$. Thus, in order to get the classification according to the Galois group, we only have to identify the representation and the conjugation class of its image in $\mathrm{GL}(k, \mathbb{F}_p)$. We find that, when $k = \ell$ or $k = 4$, the Galois group of the normal closure of an extension of degree p^k having no intermediate fields is of type $(\mathbb{F}_p)^k \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^k}^*$, or of type $(\mathbb{F}_p)^k \rtimes Z$, where Z is a non abelian subgroup of $\mathbb{F}_{p^k}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$; if $k = 4$ the Galois group can also be of type $(\mathbb{F}_p)^4 \rtimes B$, where B is a subgroup of $(\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*/\mathbb{F}_p^*) \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ (where $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acts non trivially only on the first factor). These are the only groups that can appear as Galois group of the normal closure of a p^k-extension with no intermediate fields.

Finally, as a further application of the correspondence theorem, we determine the ramification groups and the discriminant of the composite of all extensions of degree p^ℓ of K having no intermediate fields using the fact, proved in Section 2.4, that this composite is equal to a certain Kummer extension of F.

Chapter 1

Preliminaries

We report some basic concepts which have a leading role in the thesis. In particular, in the first two sections we present the objects and in the third one the tools to attack the problem faced in this thesis, that is to classify the isomorphism classes of extensions of degree a power of p of a p-adic field.

1.1 Basic properties of extensions of local fields

Let F be a field. An *exponential valuation* on F is a map $v\colon F \longrightarrow \mathbb{R}\cup\{\infty\}$ satisfying the properties

- $v(\alpha) = \infty \;\Leftrightarrow\; \alpha = 0$,
- $v(\alpha\beta) = v(\alpha) + v(\beta)$,
- $v(\alpha+\beta) \geq \min\{v(\alpha), v(\beta)\}$,

where we fix the following conventions regarding elements $a \in \mathbb{R}$ and the symbol ∞: $a < \infty$, $a + \infty = \infty$, $\infty + \infty = \infty$. Note that if $v(\alpha) \neq v(\beta)$ then $v(\alpha+\beta)$ is always equal to $\min\{v(\alpha), v(\beta)\}$.
If F is equipped with such a function, it will be said a *valued field*.
From now on, we will say *valuation* to intend *exponential valuation*. Two valuations v_1 and v_2 on F are called *equivalent* if $v_1 = sv_2$, for some real number $s > 0$.
The subset $\mathcal{O}_F = \{\alpha \in F \mid v(\alpha) \geq 0\}$ is a ring, called the *valuation ring* of F, with group of units $\mathcal{O}_F^* = \{\alpha \in F \mid v(\alpha) = 0\}$ and the unique maximal ideal $\mathfrak{p}_F = \{\alpha \in F \mid v(\alpha) > 0\}$. $\mathcal{O}_F$ is an integral domain with field of fractions F; the

field $\mathcal{O}_F/\mathfrak{p}_F = \kappa_F$ is called the *residue class field* of $\mathcal{O}_F$. If $v(F^*) = \{0\}$ we call v the *trivial valuation* and if the value group $v(F^*)$ admits a smallest positive value s we say that v is *discrete*; in this case one finds $v(F^*) = s\mathbb{Z}$. It is called *normalized* if $s = 1$. Dividing by s we may always pass to a normalized valuation without changing the invariants $\mathcal{O}_F$, $\mathcal{O}_F^*$, $\mathfrak{p}_F$. Having done so, an element $\pi \in \mathcal{O}_F$ such that $v(\pi) = 1$ is a *prime element* or a *uniformizer*, and every element $\alpha \in F^*$ admits a unique representation $\alpha = u\pi^m$ with $m \in \mathbb{Z}$ and $u \in \mathcal{O}_F^*$. Moreover the nonzero ideals of $\mathcal{O}_F$ are given by $\mathfrak{p}_F^n = \pi^n\mathcal{O}_F = \{\alpha \in F \mid v(\alpha) \geq n\}$ for $n \geq 0$.
A sequence $(\alpha_n)_{n\geq 0}$ of elements of F is called a *Cauchy sequence* if for each $c \in \mathbb{R}$ there exists an $n_0 \geq 0$ such that $v(\alpha_n - \alpha_m) \geq c$ for $m, n \geq n_0$. It coincides with the usual definition in a metric space when F is equipped with the distance induced by the norm defined as $|\alpha| = \varepsilon^{v(\alpha)}$, for some fixed $\varepsilon \in (0, 1)$. Thus a valuation induces a topology on F, for which a system of neighbourhoods of 0 is given by the powers $\mathfrak{p}_F^n$, for $n \geq 1$, of the maximal ideal, while a basis of neighbourhoods of the element 1 of F^* is the filtration $\mathcal{O}_F^* = U_{F,0} \supseteq U_{F,1} \supseteq U_{F,2} \supseteq \cdots$ of subgroups $U_{F,n} = 1 + \mathfrak{p}_F^n$ of $\mathcal{O}_F^*$. $U_{F,n}$ is called the n-th *higher unit group* and $U_{F,1}$ the group of *principal units*.

Proposition 1.1. *The following facts hold:*

1. $U_{F,0}/U_{F,1} \simeq \kappa_F^*$,
2. *for $i \geq 1$, the group $U_{F,i}/U_{F,i+1}$ is canonically isomorphic to the group $\mathfrak{p}_F^i/\mathfrak{p}_F^{i+1}$, which is itself isomorphic to the additive group of κ_F.*

Proof. They are both simple proofs.

1. The isomorphism is induced by the canonical and obviously surjective homomorphism

$$\begin{array}{rcl} \mathcal{O}_F^* = U_{F,0} & \longrightarrow & \kappa_F^* \\ u & \longmapsto & u \pmod{\mathfrak{p}_F} \end{array}$$

   the kernel of which is $U_{F,1}$.

2. Consider the homomorphism that maps each $\alpha \in \mathfrak{p}_F^i$ to the element $1 + \alpha$ in $U_{F,i}$; this gives, by passing to the quotient, the canonical isomorphism. Moreover $\mathfrak{p}_F^i/\mathfrak{p}_F^{i+1}$ is a one-dimensional vector space over κ_F, so it is isomorphic to κ_F as an additive group. □

When the field F will be fixed, we will omit the subscript F in $U_{F,i}$ and we will write only U_i for the i-th higher unit group.

A valued field (F, v) is called *complete* if every Cauchy sequence $(\alpha_n)_{n\geq 0}$ in F converges to an element $a \in F$. From any valued field (F, v) we get a complete valued field $(\widehat{F}, v)$ by the process of completion: take the ring R of all Cauchy sequences of (F, v), consider therein the maximal ideal $\mathfrak{m}$ of all nullsequences with respect to v, and define $\widehat{F} = R/\mathfrak{m}$. One embeds the field F into $\widehat{F}$ by sending every $a \in F$ to the class of the constant Cauchy sequence $(a, a, a, \dots)$; the valuation v is extended from F to $\widehat{F}$ by giving the element $a \in \widehat{F}$, which is represented by the Cauchy sequence $(a_n)_{n\geq 0}$, the valuation $v(a) = \lim_n v(a_n)$.

Let F be a field which is complete with respect to the valuation v and let $f \in \mathcal{O}_F[X]$ be a primitive polynomial, i.e. $f(X) \not\equiv 0 \pmod{\mathfrak{p}_F}$. Then the following holds

Lemma 1.2 (Hensel). *If $f \in \mathcal{O}_F[X]$ admits modulo $\mathfrak{p}_K$ a factorization*

$$f(X) \equiv \bar{g}(X)\bar{h}(X) \pmod{\mathfrak{p}_F}$$

into relatively prime polynomials $\bar{g}, \bar{h} \in \kappa_F[X]$, then $f(X)$ admits a factorization

$$f(X) = g(X)h(X)$$

into polynomials $g, h \in \mathcal{O}_F[X]$ such that $\deg(g) = \deg(\bar{g})$ and

$$g(X) \equiv \bar{g}(X) \pmod{\mathfrak{p}_F} \quad \textit{and} \quad h(X) \equiv \bar{h}(X) \pmod{\mathfrak{p}_F}.$$

Proof. See [Neu99, Chap. II, §4]. □

Remark. Hensel's lemma is valid in a much bigger class of valued fields than the complete ones. A field satisfying Hensel's lemma is called *henselian field*.

A complete discretely valued field with perfect residue field is often referred to as a *local field*. Moreover a local field is often assumed to be locally compact. It turns out that F is locally compact if and only if it is complete and the residue field κ_F is a finite field. Hence we will assume that a local field is a complete discretely valued field which is locally compact and having a fixed prime p as the characteristic of the residue field.

We will denote by f_F the absolute residual degree $[\kappa_F : \mathbb{F}_p]$, which is called *absolute inertia degree*, and we will set $e_F = v(p)$, which is called *absolute ramification index*.

Proposition 1.3. *The multiplicative group of a local field F can be decomposed as*

$$F^* \simeq \langle \pi \rangle \times \kappa_F^* \times U_{F,1}$$

where π is a uniformizer of F, $\langle \pi \rangle = \{\pi^k \mid k \in \mathbb{Z}\}$ and $U_{F,1} = 1 + \mathfrak{p}_F$ is the group of principal units.

Proof. For every $\alpha \in F^*$, one has a unique representation $\alpha = \pi^n u$ with $n \in \mathbb{Z}$ and $u \in \mathcal{O}_F^*$, so that $F^* \simeq \langle \pi \rangle \times \mathcal{O}_F^*$.
Let $q = |\kappa_F|$ be the cardinality of κ_F, so that κ_F^* is isomorphic to the group of $(q-1)$-th roots of unity. Since the polynomial $X^{q-1} - 1$ splits into linear factors over F by Hensel's lemma, $\mathcal{O}_F^*$ contains the group of $(q-1)$-th roots of unity. This implies that the homomorphism $\mathcal{O}_F^* = U_{F,0} \longrightarrow \kappa_F^*$ has a section and hence by 1 of 1.1, it follows that $\mathcal{O}_F^* = U_{F,0} \simeq \kappa_F^* \times U_{F,1}$. □

If F is a local field with valuation v_F, then v_F may be extended in a *unique way* to a valuation v_L of any given algebraic extension L/F. When L/F has finite degree n, this extension is given by the formula

$$v_L(\alpha) = \frac{1}{n} v_F(N_{L/F}(\alpha)),$$

where $N_{L/F}$ is clearly the norm map. In this case L is again a local field.
For the value groups and residue class fields of v_F and v_L, one gets the inclusions $v_F(F^*) \subseteq v_L(L^*)$ and $\kappa_F \subseteq \kappa_L$. The index $e = e(L/F) = (v_L(L^*) : v_F(F^*))$ is called the *ramification index* of the extension L/F and the degree $f = f(L/F) = [\kappa_L : \kappa_F]$ is called the *inertia degree*. Since v_F (and v_L) is discrete (not necessarily normalized), because F (and L) is local, and if π (respectively Π) is an element of smallest value of F (respectively L), then one has $e = (v_L(\Pi)\mathbb{Z} : v_F(\pi)\mathbb{Z})$, so that $v_F(\pi) = v_L(\pi) = e v_L(\Pi)$ and $\pi = \varepsilon \Pi^e$, for some unit $\varepsilon \in \mathcal{O}_L^*$.

Proposition 1.4. *If L/F is a finite extension of local fields, then*

$$[L : F] = ef.$$

Proof. See [Neu99, Prop 6.8, chap. II]. □

A finite extension of local fields L/F is called *unramified* if $[L : F] = [\kappa_L : \kappa_F] = f$, i.e. $e = 1$. In general, if L/F is an extension of local fields, the composite T/F of

all unramified subextensions is called the *maximal unramified subextension* of L/F. Its residue class field is κ_L and its value group is equal to that of F.

L/F is called *tamely ramified* if $([L:T],p)=1$, i.e. $(e,p)=1$. This happens if and only if the extension L/T is generated by radicals $L=T(\sqrt[m_1]{a_1},\dots,\sqrt[m_r]{a_r})$ such that $(m_i,p)=1$ (see [Neu99, chap. II]). The composite V/F of all tamely ramified subextensions of an extension of local fields L/F is called the *maximal tamely ramified* subextension of L/F. Its value group is the subgroup $v_L(L^*)^{(p)}$ of $v_L(L^*)$ which consists of all elements ω such that $m\omega \in v_F(F^*)$ with $(m,p)=1$; its residue class field is κ_L.

Therefore, for every finite extension of local fields L/F, one has the following splits:

$$\begin{array}{ccccccc} F & \subseteq & T & \subseteq & V & \subseteq & L \\ \kappa_F & \subseteq & \kappa_L & = & \kappa_L & = & \kappa_L \\ v_F(F^*) & = & v_L(T^*) & \subseteq & v_L(L^*)^{(p)} & \subseteq & v_L(L^*) \end{array}$$

If $e=e'p^a$ where $(e',p)=1$, then $[V:T]=e'$. The extension L/F is called *totally ramified* if $T=F$, and *wildly ramified* if it is not tamely ramified, i.e. if $V\neq L$. A totally ramified extension can always be generated by an Eisenstein equation $X^e+a_{e-1}X^{e-1}+\cdots+a_0=0$ where $a_i\in\mathfrak{p}_F$ for all i and $a_0\neq 0 \pmod{\mathfrak{p}_F^2}$. If the extension is also tame, then it can be generated by a root of the equation $X^e-\pi_F=0$ (see [Lan94, Prop 11-12, chap. II]).

Let L/F be a Galois extension of local fields, and let $G=\mathrm{Gal}(L/F)$ be its Galois group; G acts on the ring $\mathcal{O}_L$. For every integer $i\geq -1$, we define the *i-th ramification group* of L/F by

$$G_i=G_i(L/F)=\{\sigma\in G \mid v_L(\sigma\alpha-\alpha)\geq i+1 \text{ for all } \alpha\in\mathcal{O}_L\}.$$

The G_i's form a decreasing sequence of normal subgroups of G; $G_{-1}=G$, G_0 is called the *inertia subgroup* of G, and $G_i=\{1\}$ for i sufficiently large.

The quotient G/G_0 is the Galois group $\mathrm{Gal}(\kappa_L/\kappa_F)$ of the residue extension, which is isomorphic to $\mathrm{Gal}(T/F)$, therefore G_0 corresponds via Galois theory to the maximal unramified subextension of L/F. G_1 is the unique p-Sylow subgroup of G_0 and G/G_1 is isomorphic to $\mathrm{Gal}(V/F)$, therefore G_1 corresponds via Galois theory to the maximal tamely ramified subextension of L/F. The quotients G_i/G_{i+1} satisfy the following

Proposition 1.5. *For $i \geq 0$, the map which, to $\sigma \in G_i$, assigns $\sigma(\pi_L)/\pi_L$, induces by passage to the quotient an isomorphism θ_i of the quotient group G_i/G_{i+1} onto a subgroup of the group $U_{L,i}/U_{L,i+1}$. This isomorphism is independent of the choice of uniformizer π_L.*

Proof. See [Ser78, Prop 7, chap. IV]. □

1.2 Basics on linear representation theory

Let F be a field, V be a vector space of finite dimension over F, and $\mathrm{GL}(V)$ be the group of isomorphisms of V onto itself. An element a of $\mathrm{GL}(V)$ is, by definition, a linear mapping of V into V which has an inverse a^{-1}; this inverse is linear. If $\dim_F V = n$, choosing a basis of V, we can identify $\mathrm{GL}(V)$ with $\mathrm{GL}(n, F)$, the group of invertible square matrices of order n and entries in F.

Definition 1.1. *A* linear representation *of G in V is a homomorphism $\rho\colon G \longrightarrow \mathrm{GL}(V)$.*

When ρ is given, we say that V is a *representation space* of G (or even simply, by abuse of language, a *representation* of G). If $\sigma \in G$, $\rho(\sigma)$ is an endomorphism of V and so its trace is defined. The function

$$\chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma))$$

is a *class function* on G (a function $f\colon G \to F$ is a class function if $f(\sigma\tau\sigma^{-1}) = f(\tau)$ for all $\sigma, \tau \in G$) called the *character* of the representation ρ. The integer $\chi_\rho(1)$, equal to the dimension of V, is called the *degree* of ρ.
Every representation ρ of G determines a representation $\tilde{\rho}$ of the F-algebra $F[G]$ (i.e. a homomorphism of F-algebras from $F[G]$ to $\mathrm{End}_F(V)$) by linear extension, that is $\tilde{\rho}(\sum a_g g) = \sum a_g \rho(g)$; on the other hand, every representation of $F[G]$ determines a representation of G by restriction. Note that to give a representation of $F[G]$ in V is the same as to define a structure of $F[G]$-module on V, i.e. a "multiplication" $\bullet$ of V by the elements of $F[G]$ which $\forall v \in V,\ \lambda \in F,\ a, b \in F[G]$ satisfies the following conditions:

1. $1 \bullet v = v$
2. $\lambda \bullet v = \lambda v$

3. $\bullet$ is F-bilinear

4. $a \bullet (b \bullet v) = (ab) \bullet v$.

For a G-module we will mean a (left) $F[G]$-module. So we will indiscriminately use the terminology "G-module" or "representation of G" to indicate the same structure on a given vector space V.
Let $\rho\colon G \longrightarrow \mathrm{GL}(V)$ be a linear representation and let W be a vector subspace of V. Suppose that W is stable under the action of G defined by ρ, then $\rho^W : G \longrightarrow \mathrm{GL}(W)$ is a linear representation of G in W, called a *subrepresentation* of ρ.
We say that $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is *irreducible* or *simple* if V is not 0 and if no vector subspace of V is stable under G, except of course 0 and V. A representation of degree 1 is clearly irreducible.

Proposition 1.6. *If G is abelian, then all the irreducible representations of G have degree* 1.

Proof. See [Ser77, Th 9, chap. III]. □

A basic result in representation theory is the following

Proposition 1.7 (Schur's lemma)**.** *Let $\rho^1\colon G \longrightarrow \mathrm{GL}(V_1)$ and $\rho^2\colon G \longrightarrow \mathrm{GL}(V_2)$ be two irreducible representations of G, and let f be a linear mapping of V_1 into V_2 such that $\rho^2(s) \circ f = f \circ \rho^1(s)$ for all $s \in G$. Then:*

- *if ρ^1 and ρ^2 are not isomorphic, we have $f = 0$;*
- *if $V_1 = V_2$ and $\rho^1 = \rho^2$, f is a homothety (i.e., a scalar multiple of the identity).*

Proof. See [Ser77, Prop 4, chap. II]. □

Let $\rho\colon G \longrightarrow \mathrm{GL}(V)$ be a representation of G, H be a subgroup of G, and ρ_H be the restriction of ρ to H. Let W be a subrepresentation of ρ_H, $\theta\colon H \longrightarrow \mathrm{GL}(W)$ be the representation of H in W thus defined. Let $s \in G$; the vector space $\rho(s)W$ depends only on the left coset sH of s; indeed, if we replace s by st, with $t \in H$, then we have $\rho(st)W = \rho(s)\rho(t)W = \rho(s)W$ since $\rho(t)W = W$. Therefore, if σ is a left coset of H in G, we can define a subspace σW of V to be $\rho(s)W$ for any $s \in \sigma$. It is clear that the σW are permuted among themselves by the $\rho(s)$, $s \in G$. Their sum $\sum_{\sigma \in G/H} \sigma W$ is thus a subrepresentation of V. We say that the representation

ρ of G in V is *induced* by the representation θ of H in W if V is equal to the sum of the σW ($\sigma \in G/H$) and if this sum is direct (that is, if $V = \bigoplus_{\sigma \in G/H} \sigma W$). In any case, the induced subrepresentation is denoted by $\mathrm{Ind}_H^G(W)$.

1.3 The correspondence theorem

In this section we state a theorem, first proved by Roberto Dvornicich, which reduces the problem of counting isomorphism classes of extensions of degree p^k of a p-adic field K having no intermediate fields to that of counting representations of dimension k of a certain group acting on a suitable vector space.
The advantage of doing this is due to the fact that the special properties of the group allows us to easily identify its representation in the fixed vector space and, as a consequence, to easily count their number.
Let F be the composite of all normal and tame extensions of K whose Galois group is a subgroup of $\mathrm{GL}(k, \mathbb{F}_p)$ and let $H = \mathrm{Gal}(F/K)$.

Theorem 1.8. *There exists a natural one-to-one correspondence between the isomorphism classes of extensions of K of degree p^k ($k \geq 1$) having no intermediate extensions and the irreducible H-submodules of F^*/F^{*p} of dimension k of the Galois module F^*/F^{*p}. The isomorphism class $[L/K]$ corresponds to Ξ where $LF = F(\sqrt[p]{\Xi})$, and $\mathrm{Gal}(LF/K)$ is always a split extension of $\mathrm{Gal}(F/K)$.*

Proof. See [DCDM, Th 3.2]. □

In order to apply the correspondence Theorem 1.8, we have to know the structure of F^*/F^{*p} as $\mathbb{F}_p[H]$-module. This is equivalent to be able to identify the irreducible representations of H contained in the $\mathbb{F}_p$-vector space F^*/F^{*p}.
Note that H is the Galois group of a finite tame extension, therefore it has the following form

$$\langle v, \tau \mid v^{-1}\tau v = \tau^q, \tau^e = 1, v^f = \tau^r \rangle$$

where $e := e_{F/K}$, $f := f_{F/K}$, $q := p^{f_K}$ and r is the smallest positive integer such that $v^f = \tau^r$ (see [Iwa55]). Moreover the extension F/K is always contained in a split one, i.e. in a tame extension whose Galois group is a semidirect product of the inertia subgroup and its complement. Since this tame split extension is of degree prime to p and unramified over F, the correspondence theorem still holds if we put

this extension in place of F (we will see this in the next chapter in the special case in which k is a prime number). Abusing notation, we continue to denote by F this split tame extension of K and by H its Galois group over K.
So we can suppose that $H = H_0 \rtimes U$ where $H_0 = \langle \tau \rangle$ and $U = \langle v \rangle$ are cyclic of order e and f respectively, $(e, p) = 1$, $e \mid q^f - 1$ and v acts on H_0 via the map $x \mapsto x^q$. This particular form of H allows us to easily describe its representations. First of all, we can observe that to study the irreducible representation ρ of $H_0 \rtimes U$, one can study the irreducible representation $\bar{\rho}$ of $\bar{H}_0 \rtimes U$, where $\bar{H}_0 = H_0/\ker(\rho_{|H_0})$, that is to say the representations of H that are faithful on the first factor. The following Lemma describes them.

Lemma 1.9. *Every irreducible representation V over $\mathbb{F}_p$ of $\langle \nu \rangle \rtimes_\mu \langle \eta \rangle$, where $\mu(\eta)$ is the elevation to p^f, that is faithful on $\langle \nu \rangle$ is the sum of the conjugates of an irreducible representation over $\overline{\mathbb{F}}_p$. Each of these is induced from a 1-dimensional representation of $\langle \nu \rangle \times \langle \eta_c \rangle$, where $\langle \eta_c \rangle = C_{\langle \eta \rangle}(\langle \nu \rangle)$ is the centralizer of $\langle \nu \rangle$ in $\langle \eta \rangle$.*
Moreover, if ν and η_c act as multiplication by α and β respectively, then the following equation holds:

$$\dim_{\mathbb{F}_p} V = \operatorname{lcm}\left(\frac{rw}{(r,f)}, r\right), \tag{1.1}$$

where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Proof. See for example [DCDM, §4.1]. □

For convenience, we now describe in more details the irreducible representations of H over $\mathbb{F}_p$.
By Lemma 1.9, all irreducible representations of $H_0 \rtimes U$ in a $\overline{\mathbb{F}}_p$-vector space faithful on the first factor are induced from 1-dimensional representations of the abelian group $H_0 \times \tilde{U}$, where $\tilde{U} = \langle \tilde{v} \rangle$ is the centralizer of H_0 in U. In particular, if $\rho\colon H_0 \rtimes U \longrightarrow \mathrm{GL}(W)$ is an irreducible representation (faithful on the first factor), then $\rho = \mathrm{Ind}_{H_0 \times \tilde{U}}^{H_0 \rtimes U}(W_\chi)$ where W_χ is a 1-dimensional $\overline{\mathbb{F}}_p$-subspace of W on which $H_0 \times \tilde{U}$ acts by the character χ. Moreover, if $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{v})$ then there is a basis of

W with respect to which τ and v act on W via the matrices

$$T_\alpha = \begin{pmatrix} \alpha & & & & \\ & \alpha^q & & & \\ & & \alpha^{q^2} & & \\ & & & \ddots & \\ & & & & \alpha^{q^{u-1}} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & & & & \beta \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{pmatrix}$$

where u is the index of $\tilde{U}$ in U.

It is easy to see that conjugate characters lead to the same representation on W.

Now, the second step is to pass from the irreducible representations over $\overline{\mathbb{F}}_p$ to the irreducible representations over $\mathbb{F}_p$. Again by Lemma 1.9, if φ is an irreducible representation of $H_0 \rtimes U$ over an $\mathbb{F}_p$-vector space V (faithful on the first factor), then it is the sum of the conjugates of an irreducible representation over $\overline{\mathbb{F}}_p$ which, as written above, is induced from a 1-dimensional one, and one has

$$\dim_{\mathbb{F}_p} V = \operatorname{lcm}\left(\frac{rw}{(r, f_K)}, r\right) \tag{1.2}$$

where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Finally it remains to identify the irreducible representations of $H_0 \rtimes U$ over the $\mathbb{F}_p$-vector space F^*/F^{*p}. For what we have said above, we first identify those over the $\overline{\mathbb{F}}_p$-vector space $F^*/F^{*p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ obtained from F^*/F^{*p} by extension of scalars and then we recover from these the irreducible $\mathbb{F}_p$-representations over F^*/F^{*p}. If π is a uniformizer of F and U_1 denotes the group of principal units of F, then from 1.3 we have

$$F^* \simeq \langle \pi \rangle \times \kappa_F^* \times U_1$$

as H-modules. It follows that

$$F^*/F^{*p} \simeq \langle \pi \rangle / \langle \pi \rangle^p \times U_1/U_1^p$$

as $\mathbb{F}_p[H]$-modules.

Recall that U_1 has a filtration $\{U_i\}_{i \geq 1}$, where $U_i = \{x \in F^* | x \equiv 1 (\mathrm{mod}\ \pi^i)\}$. It induces the filtration $\{U_i U_1^p / U_1^p\}_{i \geq 1}$ of U_1/U_1^p and, as U_{i+1} is complemented in U_i as H-module, also $U_{i+1}U_1^p/U_1^p$ is complemented in $U_i U_1^p/U_1^p$ as $\mathbb{F}_p[H]$-module ([DCDM, Prop 4.3]). Therefore one has

$$F^*/F^{*p} \simeq \langle \pi \rangle / \langle \pi \rangle^p \oplus \bigoplus_{i=1}^{\infty} U_i U_1^p / U_{i+1} U_1^p.$$

The nonzero terms in the right-hand side are those with $i = pe_F/(p-1)$ and, $0 < i < pe_F/(p-1)$ with $(i,p) = 1$ (see for example [FV02]). Then the above relation can be written as

$$F^*/F^{*p} \simeq \langle\pi\rangle/\langle\pi\rangle^p \oplus \bigoplus_{i\in[\![0,I_F]\!]} U_iU_1^p/U_{i+1}U_1^p \oplus U_{I_F}U_1^p/U_1^p,$$

where $I_F = pe_F/(p-1)$ and $[\![0,I_F]\!]$ is the set of integers prime to p in the interval $]0,I_F[$.

We want to describe the representations of H contained in F^*/F^{*p}. To do this, observe that the action of H on $\langle\pi\rangle/\langle\pi\rangle^p \simeq \mathbb{F}_p$ is clearly trivial and that $U_{I_F}U_1^p/U_1^p$ corresponds via Kummer theory to the Galois unramified extension of degree p, so the action of H on this submodule of dimension 1 of F^*/F^{*p} is given by the cyclotomic character ω. Since we are interested in the irreducible subrepresentations of dimension $k \geq 2$, we can reduce to consider those contained in $\bigoplus_{i\in[\![0,I_F]\!]} U_iU_1^p/U_{i+1}U_1^p$.

We need to study the structure of $U_iU_1^p/U_{i+1}U_1^p$ as $\mathbb{F}_p[H]$-module. Since F/K is a tamely ramified extension, we can choose as a uniformizer π of F an e-th root of a uniformizer of K, where clearly $e = e_{F/K}$. Then for $i \geq 1$, each element of U_i/U_{i+1} can be written as $1+\epsilon\pi^i$ with $\epsilon \in U_0$ ($U_0 = \mathcal{O}_F^*$ is the multiplicative group of the ring of the integers of F). The action of H on it is given by

$$\tau(1+\epsilon\pi^i) = 1+\zeta^i\epsilon\pi^i+\ldots, \qquad v(1+\epsilon\pi^i) = 1+\epsilon^q\pi^i+\ldots,$$

where $\zeta = \tau(\pi)/\pi$ is a primitive e-th root of 1. By Proposition 1.1, one can identify U_i/U_{i+1} with the additive group of κ_F via the map

$$1+\epsilon\pi^i \mapsto \bar{\epsilon}$$

and this induces on κ_F the following action of H

$$\tau(\bar{\epsilon}) = \bar{\zeta}^i\bar{\epsilon}, \qquad v(\bar{\epsilon}) = \bar{\epsilon}^q.$$

Denote by M_i the $\mathbb{F}_p[H]$-module formed by the $\mathbb{F}_p$-module κ_F with the above action of H. Since $U_i/U_{i+1} \simeq U_iU_1^p/U_{i+1}U_1^p$ as H-modules, it is clear that

$$U_iU_1^p/U_{i+1}U_1^p \simeq M_i$$

as $\mathbb{F}_p[H]$-modules. In other words, we can write the following isomorphism of $\mathbb{F}_p[H]$-modules

$$F^*/F^{*p} \simeq \mathbb{F}_p \oplus \bigoplus_{i\in[\![0,I_F]\!]} M_i \oplus M_\omega, \tag{1.3}$$

where M_ω corresponds to the unramified extension of degree p. We search the irreducible $\mathbb{F}_p[H]$-submodules of $\bigoplus_{i\in[\![0,I_F]\!]} M_i$ or, equivalently, the irreducible representations of H over $\mathbb{F}_p$ contained in $\bigoplus_{i\in[\![0,I]\!]} M_i$ (viewed as $\mathbb{F}_p$-vector space). To do this we first extend the $\mathbb{F}_p$-representation M_i of H to an $\overline{\mathbb{F}}_p$-representation, we identify its $\overline{\mathbb{F}}_p$ subrepresentations and from each of these we find the $\mathbb{F}_p$ subrepresentations via the sum of its conjugates.
Let $\overline{M}_i = M_i \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ be the $\overline{\mathbb{F}}_p[H]$-module obtained from M_i by extension of scalars to the algebraic closure of $\mathbb{F}_p$. It can be shown that

$$\overline{M}_i \simeq (\mathrm{Ind}_{H_0}^{H}(V_\alpha))^{f_K}$$

where V_α is the $\overline{\mathbb{F}}_p[H_0]$-module of dimension 1 on which τ acts as multiplication by $\alpha = \zeta^i$ and ζ is a fixed primitive e-th root of unity (see [DCDM, Prop 4.5]).
Recall that we denoted by $\tilde{U}$ the centralizer of H_0 in U, and consider first

$$\mathrm{Ind}_{H_0}^{H_0\times\tilde{U}}(V_\alpha) = \overline{\mathbb{F}}_p[\tilde{U}] \otimes_{\overline{\mathbb{F}}_p} V_\alpha.$$

Recall also that $\tilde{U}$ is generated by $\tilde{v} = v^u$ of order f/u, so the above representation can be written as

$$\mathrm{Ind}_{H_0}^{H_0\times\tilde{U}}(V_\alpha) = \bigoplus_{i=1}^{f/u} \tilde{v}^i V_\alpha = \bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p \\ \beta^{f/u}=1}} V_{(\alpha,\beta)},$$

where $V_{(\alpha,\beta)}$ is the representation of dimension 1 such that τ and $\tilde{v}$ act via multiplication by α and β respectively. Consequently, we have

$$\begin{aligned}
\mathrm{Ind}_{H_0}^{H}(V_\alpha) &= \mathrm{Ind}_{H_0\times\tilde{U}}^{H}(\mathrm{Ind}_{H_0}^{H_0\times\tilde{U}}(V_\alpha)) \\
&= \mathrm{Ind}_{H_0\times\tilde{U}}^{H} \bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p \\ \beta^{f/u}=1}} V_{(\alpha,\beta)} \\
&= \bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p \\ \beta^{f/u}=1}} \mathrm{Ind}_{H_0\times\tilde{U}}^{H}(V_{(\alpha,\beta)}).
\end{aligned}$$

Denote $\mathrm{Ind}_{H_0\times\tilde{U}}^{H}(V_{(\alpha,\beta)})$ as $J_{(\alpha,\beta)}$, then

$$\begin{aligned}\overline{M}_i &\simeq \left(\bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p\\ \beta^{f/u}=1}} J_{(\alpha,\beta)}\right)^{f_K}\\ &\simeq \bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p\\ \beta^{f/u}=1}} {J_{(\alpha,\beta)}}^{f_K}. \end{aligned} \tag{1.4}$$

Let $Y=\bigoplus_{i\in[\![0,I_F]\!]}\overline{M}_i$; then $J_{(\alpha,\beta)}$ appears $n_K=[K:\mathbb{Q}_p]$ times in Y. In fact, the i's such that $\zeta^i=\alpha$ have equal remainder modulo e; being $(e,p)=1$, those ones in $]0,I_F[$ and prime to p are exactly e_K. Multiplying by the exponent of $J_{(\alpha,\beta)}$ that appears in (1.4), we have the claim.

Moreover, if s is the dimension of $J_{(\alpha,\beta)}$ then the s conjugate pairs (α^{q^i},β) yield the same representation, therefore the multiplicity of $J_{(\alpha,\beta)}$ in Y is sn_K.

It is easy to see that the representation $J_{(\alpha,\beta)}$ has

$$d=\mathrm{lcm}(w,(r,f_K))$$

conjugates over $\mathbb{F}_p$, where $r=[\mathbb{F}_p(\alpha):\mathbb{F}_p]$ and $w=[\mathbb{F}_p(\beta):\mathbb{F}_p]$ as above. In fact $J_{(\alpha,\beta)}$ is clearly stabilized by $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p(\alpha,\beta))$ and by the powers of the Frobenius ϕ_q fixing β (since $\phi_q(\rho(\tau))=\rho(\tau)$). Now, in $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ the group generated by ϕ_q is equal to the group generated by $\phi_{p^{(r,f_K)}}$ since $\mathrm{o}(\phi_p^{f_K})=\mathrm{o}(\phi_p^{(r,f_K)})$, therefore the smallest power of $\phi_{p^{(r,f_K)}}$ fixing $\mathbb{F}_p(\beta)$ is $\phi_{p^{\mathrm{lcm}(w,(r,f_K))}}$, which then generates the stabilizer of $J_{(\alpha,\beta)}$.

It follows that $J_{(\alpha,\beta)}$ is defined over $D=\mathbb{F}_{p^d}$, where $d=\mathrm{lcm}(w,(r,f_K))$, and has d conjugates over $\mathbb{F}_p$. Moreover, a short reflection leads to observe that the dimension s of $J_{(\alpha,\beta)}$ is equal to $\frac{r}{(r,f_K)}$ since v acts on τ as elevation to q and therefore s is the smallest power of q such that $e\mid q^s-1$, i.e. the order of q in $(\mathbb{Z}/e\mathbb{Z})^*$.

Recall that we want to identify the irreducible subrepresentations of Y defined over $\mathbb{F}_p$: they are sum of the conjugates of $J_{(\alpha,\beta)}$ as α and β vary through suitable roots of unity.

Let X be an irreducible subrepresentation of Y defined over $\mathbb{F}_p$ and containing a unique copy of $J_{(\alpha,\beta)}$. From each copy of $J_{(\alpha,\beta)}$ contained in Y and defined over D, we obtain a representation isomorphic to X. Consequently, to count the subrepresentations isomorphic to X and defined over $\mathbb{F}_p$ is the same as to count the

subrepresentations that are isomorphic to $J_{(\alpha,\beta)}$ and defined over D. This can be made by counting the subrepresentations contained in $(J_{(\alpha,\beta)})^{sn_K}$ and working over D. Consider the embeddings

$$J_{(\alpha,\beta)} \longrightarrow (J_{(\alpha,\beta)})^{sn_K}$$

which are defined over D. Using Schur's Lemma 1.7, we find that the number of embeddings is $|D|^{sn_K} - 1$ and this number must be divided by $|D| - 1$ when taking into account that two immersions have the same image if and only if they differ by multiplication by a constant. It follows that the number of representations defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is

$$\frac{p^{dsn_K} - 1}{p^d - 1}. \tag{1.5}$$

Chapter 2

Extensions of degree p^ℓ

2.1 Improving the correspondence theorem for p^ℓ extensions

We prove the correspondence theorem in the particular case in which k is equal to a prime number ℓ with a change in the definition of F. In the following version of the theorem, F is the smallest field we can take working for the correspondence. Let $F = F(K)$ be the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}_{p^\ell}^*$ or to a non abelian subgroup of $\mathbb{F}_{p^\ell}^* \rtimes_\theta \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ where $\theta(\phi_p) = \phi_p|_{\mathbb{F}_{p^\ell}^*} \in \mathrm{Aut}(\mathbb{F}_{p^\ell}^*)$ (ϕ_p is the Frobenius automorphism), and let $H = \mathrm{Gal}(F/K)$. Then

Theorem 2.1. *There exists a one-to-one correspondence between the isomorphism classes of extensions of degree p^ℓ of K having no intermediate extensions and the irreducible H-submodules of dimension ℓ over $\mathbb{F}_p$ of F^*/F^{*p}.*

Remark. Since the degree of $K(\zeta_p)$ over K divides $p-1$, we have $K(\zeta_p) \subseteq F$.

Proof. We first show that to an extension L/K of degree p^ℓ having no intermediate extensions one can associate an irreducible H-submodule of dimension ℓ of F^*/F^{*p}. In order to obtain this, we will prove that LF/F is an elementary abelian extension of degree p^ℓ. It is easy to see that $[LF : F] = p^\ell$ since L and F are linearly disjoint over K. Observe that the extension L/K cannot be unramified, because otherwise it would be abelian and hence it admits intermediate fields; in particular it is totally ramified, since otherwise it would have a proper subextension given

by the maximal unramified subextension. Let $\tilde{L}$ be the normal closure of L/K and $G = \mathrm{Gal}(\tilde{L}/K)$. As usual, G has the lower numbering ramification filtration $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}$, where for every i the subgroup G_i is normal in G and for every $i \geq 1$ the quotient G_i/G_{i+1} is an elementary abelian p-group.
Let $\tilde{H} \subseteq G$ be the subgroup fixing L. Since $\tilde{L}$ is the normal closure of L/K, no subgroup of $\tilde{H}$ is normal in G; it follows that the intersection of all its conjugates (which is normal if not trivial) is trivial. Moreover since L/K has no intermediate extensions, $\tilde{H}$ is a maximal subgroup of G and hence there is a unique t such that $G_{t+1} \subseteq \tilde{H}$ and $G_t\tilde{H} = G$; observe that we must have $t \geq 1$ since L/K is a totally and wildly ramified extension.
Now, G_t is clearly a $\tilde{H}$-module (the action being given by conjugation) and, since the centralizer $C_{\tilde{H}}(G_t)$ of G_t in $\tilde{H}$ is trivial (being contained in the intersection of all conjugates of $\tilde{H}$), it is a faithful $\tilde{H}$-module. Moreover, $G_{t+1} = \{1\}$ since $\tilde{H}$ has no subgroup normal in G, therefore G_t is an elementary abelian p-group; while, from $C_{\tilde{H}}(G_t) = \{1\}$, we have $G_t \cap \tilde{H} = \{1\}$. It follows that $G \simeq G_t \rtimes \tilde{H}$ and $|G_t| = p^\ell$. This implies that G_t is also irreducible as $\tilde{H}$-module since otherwise there would exist a proper $\tilde{H}$-submodule A of G_t and then a proper subgroup $A \rtimes \tilde{H}$ of G containing $\tilde{H}$, which is a contradiction to the maximality of $\tilde{H}$.
Let L_1 be the subfield of $\tilde{L}$ fixed by G_t, so $\mathrm{Gal}(L_1/K) \simeq \tilde{H}$. We will show that the order of $\tilde{H}$ is prime to p. Let $\tilde{H}_1$ be the ramification group of $\tilde{H}$, then either $\tilde{H}_1 = \{1\}$ or $\tilde{H}_1$ is the unique p-Sylow of $\tilde{H}_0$, and it is normal in $\tilde{H}$. But if $\tilde{H}$ has a non trivial normal p-subgroup, then G_t would have a proper $\tilde{H}$-submodule, contradicting its irreducibility. It follows that the ramified part of L_1/K has order prime to p. Moreover, also the unramified part has order prime to p since its p-Sylow subgroup would lift to a p-Sylow of $\tilde{H}$ (see Ex. 8.7 of [Ser77]) which would be normal in $\tilde{H}$ because the natural projection preserves normality, and we can conclude with the same argument of above. Therefore necessarily $p \nmid \mathrm{o}(\tilde{H})$.
Now we prove that L_1 is contained in F.
Since $p \nmid \mathrm{o}(\tilde{H})$, $\tilde{H} = \mathrm{Gal}(L_1/K)$ is the Galois group of a tame extension, therefore, as seen in Section 1.3, it is of the form

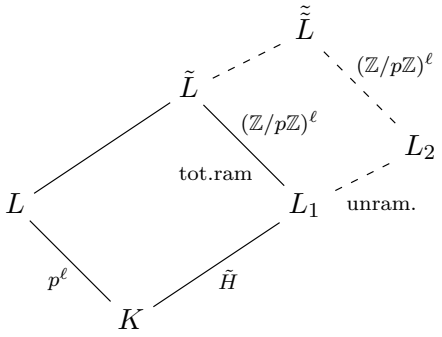
$$\langle v, \tau \mid v^{-1}\tau v = \tau^q, \tau^e = 1, v^f = \tau^r \rangle$$

where $e = e_{L_1/K}$, $f = f_{L_1/K}$, $q = p^{f_K}$ and r is the smallest positive integer such that $v^f = \tau^r$ (see [Iwa55]). Such an extension is not necessarily split, but it is always

contained in a split one, say L_2/K, i.e. in a tame extension whose Galois group is a semidirect product of the inertia subgroup and its complement. In particular we can take L_2 such that L_2/L_1 is the unramified extension of L_1 of degree $\frac{e}{(e,r)} = \mathrm{o}(v^f)$. Let $\tilde{\tilde{H}} = \mathrm{Gal}(L_2/K)$ and $\tilde{\tilde{L}} = \tilde{L}L_2$. Since $\tilde{\tilde{H}}$ is the Galois group of a split tame extension, we have

$$\tilde{\tilde{H}} = \langle\tilde{\tau}\rangle \rtimes \langle\tilde{v}\rangle$$

with $\mathrm{o}(\tilde{\tau}) = e_{L_2/K} = e_{L_1/K}$, $\mathrm{o}(\tilde{v}) = f_{L_2/K}$ and $\tilde{v}^{-1}\tilde{\tau}\tilde{v} = \tilde{\tau}^q$. The particular choice of L_2 implies that $\mathrm{Gal}(L_2/L_1) = \langle\tilde{v}^f\rangle$.



It easy to see that $\mathrm{Gal}(\tilde{\tilde{L}}/L_2) \simeq G_t \simeq (\mathbb{Z}/p\mathbb{Z})^\ell$, $\mathrm{Gal}(\tilde{\tilde{L}}/L) \simeq \tilde{\tilde{H}}$ and thus $\mathrm{Gal}(\tilde{\tilde{L}}/K) \simeq G_t \rtimes_\rho \tilde{\tilde{H}}$. This means that there exists a representation ρ of $\tilde{\tilde{H}}$ of dimension ℓ over $\mathbb{F}_p$ which factors through $\tilde{H} \simeq \tilde{\tilde{H}}/\langle\tilde{v}^f\rangle$ and the induced map $\bar{\rho}\colon \tilde{H} \to \mathrm{GL}(\ell, \mathbb{F}_p)$ must give the action of $\tilde{H}$ on G_t. ρ is irreducible, since otherwise G_t would have a proper $\tilde{H}$-submodule, but not necessarily faithful. Nevertheless, since the action of $\tilde{H}$ on G_t is faithful and L_2/L_1 being the unramified extension of L_1 degree $\frac{e}{(e,r)}$, ρ is still faithful in $\langle\tilde{\tau}\rangle$ and $\mathrm{Ker}\rho = \langle\tilde{v}^f\rangle$. In fact, since ρ factors through $\tilde{H}$, $\mathrm{Ker}\rho \supseteq \langle\tilde{v}^f\rangle$ and, since $\bar{\rho}$ is injective being the action of $\tilde{H}$ faithful on G_t, $\mathrm{Ker}\rho = \langle\tilde{v}^f\rangle$.

The advantage of passing from $\tilde{H}$ to $\tilde{\tilde{H}}$ is due to the fact that we can now use Lemma 1.9 to obtain a precise description of ρ.

By Lemma 1.9, there exist $\alpha, \beta \in \overline{\mathbb{F}}_p^*$ such that ρ is the sum of the conjugates of the representation obtained by induction from the 1-dimensional representation on which $\tilde{\tau}$ and $\tilde{v}_c$ (with $\langle\tilde{v}_c\rangle = C_{\langle\tilde{v}\rangle}(\langle\tilde{\tau}\rangle)$) act as multiplication by α and β respectively. Moreover, by equation (1.1), α and β are such that

$$\ell = \mathrm{lcm}\left(\frac{rw}{(r, f_K)}, r\right),$$

where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Therefore we must have $r = 1$ or $r = \ell$ (and also $w = 1$ or $w = \ell$). This means

that our representations over $\mathbb{F}_p$ are either the sum of the ℓ conjugates of a 1-dimensional representation defined over $\mathbb{F}_{p^\ell}$, or it is the only conjugate of an induced representation from a 1-dimensional one.
Since $\tilde{H}$ is isomorphic to $\tilde{\tilde{H}}/\ker\rho$, we are interested in the image of $\tilde{\tilde{H}}$ under ρ.
If $r = 1$ then $\alpha \in \mathbb{F}_p^*$, i.e. $e = \mathrm{o}(\tilde{\tau}) = \mathrm{o}(\alpha) \mid p-1$, therefore $\tilde{\tau}^q = \tilde{\tau}$ so that $\tilde{\tilde{H}}$ is abelian. It follows that the image of $\tilde{\tilde{H}}$ under ρ is cyclic, isomorphic to the subgroup of $\mathbb{F}_{p^\ell}^*$ generated by α and β. Therefore in this case $L_1 \subseteq F$.
If $r = \ell$, then we have to distinguish two cases: $\ell \mid f_K$ and $\ell \nmid f_K$. In the first case, we have again $\tilde{\tau}^q = \tilde{\tau}$ and hence $\tilde{\tilde{H}}$ abelian; since $r = \ell$, by the same argument of the previous case, $\tilde{H}$ is isomorphic to a subgroup of $\mathbb{F}_{p^\ell}^*$. If $\ell \nmid f_K$ then $\tilde{v}$ acts as elevation to p and $\tilde{\tilde{H}}$ is not abelian. But $\langle\tilde{\tau}\rangle \rtimes \langle\tilde{v}^\ell\rangle$ is abelian and its image under ρ is cyclic, isomorphic to the subgroup C of $\mathbb{F}_{p^\ell}^*$ generated by α and β. Moreover, the image of $\tilde{v}$ is isomorphic to the product of β by an element of order ℓ which acts as elevation to p. It follows that the image of $\tilde{\tilde{H}}$ under ρ is isomorphic to a subgroup of

$$C \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$$

with $C < \mathbb{F}_{p^\ell}^*$. Therefore again, we find that L_1 is contained in F.
It follows that $\tilde{L} = LL_1 \subseteq LF$. $\tilde{L}/L_1$ is totally and wildly ramified since L/K is, therefore $\tilde{L} \cap F = L_1$ and $\mathrm{Gal}(LF/F) \simeq G_t$. This means that LF/F is an elementary abelian extension of degree p^ℓ. Thus, by Kummer theory, $LF = F(\sqrt[p]{\Xi})$ for some subgroup Ξ of F^*/F^{*p} of dimension ℓ as $\mathbb{F}_p$-vector space. Moreover, LF/K is Galois because $LF = \tilde{L}F$ and $\tilde{L}/K$ and F/K are Galois, so Ξ is a H-module (the action of H being that induced by the action on F^*) and it is irreducible because otherwise G_t would have a proper $\tilde{H}$-submodule.
Note that the conjugates of L over K lead to the same H-module Ξ with this construction. In fact the construction of Ξ starts from the normal closure of L which is also the normal closure of all its conjugates. Thus we can define a map Ψ from the set of the isomorphism classes of p^ℓ-extensions of K having no intermediate fields to the set of the irreducible H-submodules of F^*/F^{*p} of dimension ℓ over $\mathbb{F}_p$.

Conversely, we show that each irreducible H-submodule of dimension ℓ of F^*/F^{*p} corresponds to the isomorphism class of an extension of degree p^ℓ of K having no subextensions. Note that $p \nmid \mathrm{o}(H)$ since F is the composite of normal extensions of degree prime to p.

Let Ξ be an irreducible H-submodule of F^*/F^{*p} which has dimension ℓ as vector space over $\mathbb{F}_p$. Put $M = F(\sqrt[p]{\Xi})$, then M/K is a Galois extension and $S = \mathrm{Gal}(M/F)$ is a H-module which is irreducible because Ξ is. Let $\mathfrak{G}$ be the Galois group of M/K. Since S is a normal subgroup of $\mathfrak{G}$ of order p^ℓ and $\mathfrak{G}/S \simeq H$ has order prime to p, by Schur-Zassenhaus Theorem we have $\mathfrak{G} \simeq S \rtimes H$. Let L be the fixed field of H; the fields fixed by the conjugates of H in $\mathfrak{G}$ form the isomorphism class of the extension L/K. Each of these extensions has degree p^ℓ and has no intermediate extensions. In fact, let T be such that $K \subseteq T \subseteq L$; T is the field fixed by a subgroup C of $\mathfrak{G}$, and since $L \supseteq T$ we have $C \supseteq H$. Therefore $C \simeq S_0 \rtimes H$ with $S_0 < S$, but S is irreducible as H-module so $S_0 = \{1\}$ or $S_0 = S$, i.e. $T = L$ or $T = K$.
It follows that we can define a map Φ from the set of the irreducible H-submodules of dimension ℓ of F^*/F^{*p} to the set of the isomorphism classes of p^ℓ-extensions of K having no intermediate fields.
Finally it is easily seen that Ψ and Φ are inverse to each other. □

Remark. The theory developed in Section 1.3 about the structure of F^*/F^{*p} as $\mathbb{F}_p[H]$-module holds in the present situation in which F is the smallest field we can take working for the correspondence.

2.2 The total number of isomorphism classes

Let V be an irreducible $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} of dimension ℓ. From what we have said above, viewing V as irreducible representation of H over $\mathbb{F}_p$, it is isomorphic to the sum of the conjugates over $\mathbb{F}_p$ of an irreducible representation of H over $\overline{\mathbb{F}}_p$, which we have denoted by $J_{(\alpha,\beta)}$. If $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$, by equation (1.2) we have

$$\dim_{\mathbb{F}_p} V = \mathrm{lcm}\left(\frac{rw}{(r, f_K)}, r\right) = \ell, \tag{2.1}$$

therefore $r = 1$ or $r = \ell$. It follows that $s = \frac{r}{(r,f_K)} = 1$ or $s = \ell$. We must distinguish two cases: $\ell \mid f_K$ and $\ell \nmid f_K$.

If $\ell \mid f_K$, then r and w must be equal to 1 or ℓ and at least one of them must be equal to ℓ. It follows that we have exactly $(p^\ell - 1)^2 - (p-1)^2$ possible pairs (α, β);

moreover, since $s = \frac{r}{(r,f_K)} = 1$, according to (1.5), for each of them there are $\frac{p^{\ell n_K}-1}{p^\ell-1}$ representations over $\mathbb{F}_p$ containing a representation isomorphic to $J_{(\alpha,\beta)}$. Finally, we have to take into account that the pairs $(\alpha,\beta),(\alpha^p,\beta^p),\ldots,(\alpha^{p^{\ell-1}},\beta^{p^{\ell-1}})$ lead to the same representation over $\mathbb{F}_p$.
Collecting all the informations, we find that if $\ell \mid f_K$ there are exactly

$$\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p^\ell-1}((p^\ell-1)^2-(p-1)^2)$$

isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields.

If $\ell \nmid f_K$ then equation (2.1) says that one of r and w must be 1 and the other ℓ. For $r=1$ and $w=\ell$, we have again $s = \dim J_{(\alpha,\beta)} = 1$ and $d=\ell$ therefore, for each of the $(p-1)(p^\ell-1)-(p-1)^2$ possible choices of (α,β), there are $\frac{p^{\ell n_K}-1}{p^\ell-1}$ $\mathbb{F}_p$-representations containing a representation isomorphic to $J_{(\alpha,\beta)}$, and for the same reason as above this number must be divided by ℓ. So for $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$ we have $\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p^\ell-1}(p-1)(p^\ell-p)$ irreducible representations of H of dimension ℓ over the $\mathbb{F}_p$-vector space F^*/F^{*p}.
To these we have to add those obtained from $r=\ell$ and $w=1$. In this case $s=\ell$ and $d=1$, i.e. $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$, therefore for each of the $(p^\ell-1)(p-1)-(p-1)^2$ possible pairs (α,β) there are $\frac{p^{\ell n_K}-1}{p-1}$ representations isomorphic to $J_{(\alpha,\beta)}$. This value needs to be divided by ℓ because from the definition of $J_{(\alpha,\beta)}$ one has $J_{(\alpha,\beta)} = J_{(\alpha^p,\beta)} = \cdots = J_{(\alpha^{p^{\ell-1}},\beta)}$. It follows that for $\alpha \in \mathbb{F}_{p^\ell}^*$ and $\beta \in \mathbb{F}_p^*$ there are $\frac{1}{\ell}(p^{\ell n_K}-1)(p^\ell-p)$ irreducible representations of H of dimension ℓ over F^*/F^{*p}.
Adding the two contributions one finds

$$\frac{1}{\ell}(p^{\ell n_K}-1)(p^\ell-p)+\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p^\ell-1}[(p-1)(p^\ell-1)-(p-1)^2] = \frac{1}{\ell}\frac{p^{\ell n_K}-1}{p^\ell-1}[(p^\ell-1)^2-(p-1)^2]$$

isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields.
Note that we have obtained the same number of isomorphism classes of extensions as in the case $\ell \mid f_K$.

2.3 Classifying according to the Galois group

In the previous section we have counted all the isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields. To each of them we can associate a group, that is the Galois group of the normal closure of the extensions over K. It turns out that some isomorphism classes are associated to the same group, i.e. non isomorphic p^ℓ-extensions of K may have normal closure with the same Galois group. In this section we identify all possible groups that can appear as the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields, and for each of them we count the number of isomorphism classes of extensions which are associated to it.

First of all observe that if L/K is a p^ℓ-extension having no intermediate fields and $\tilde{L}$ is its normal closure then, by Theorem 2.1,

$$\mathrm{Gal}(\tilde{L}/K) \simeq V \rtimes_{\bar{\rho}} \bar{H}$$

where $\bar{\rho}$ is the map induced on the quotient $\bar{H} = H/\ker\rho$ and the pair (V, ρ) is the representation of dimension ℓ of H in F^*/F^{*p}, which corresponds to the class of L/K under the correspondence of Theorem 2.1. In other words, $\mathrm{Gal}(\tilde{L}/K)$ is the semidirect product of V with the largest quotient of H acting faithfully on it.
Fixing a basis of the $\mathbb{F}_p$-vector space V, we can identify the image of ρ with a subgroup of $\mathrm{GL}(\ell, \mathbb{F}_p)$, so that $\mathrm{Gal}(\tilde{L}/K) \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_\rho$ where $\mathcal{H}_\rho$ represents the action of $\bar{H}$ on V given by $\bar{\rho}$, expressed with respect to the fixed basis.
Now observe that, for what we have said above, our representations are sums of the conjugates of s-dimensional representations $J_{(\alpha,\beta)}$, where $s = 1$ or $s = \ell$ and $\alpha, \beta \in \mathbb{F}_{p^\ell}^*$: if $s = 1$ then $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_{p^\ell}$ and $\bar{H}$ is abelian, so $\mathcal{H}_\rho = \mathcal{H}_{(\alpha,\beta)}$ is cyclic since it is isomorphic to the homomorphic image of a finite group in $\mathrm{GL}(1, \mathbb{F}_{p^\ell}) = \mathbb{F}_{p^\ell}^*$; if $s = \ell$ then $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$ but the group $\mathcal{H}_{(\alpha,\beta)}$ of the matrices which describes the action of $\bar{H}$ is not abelian.
The normal closures of two isomorphism classes have the same Galois group if and only if

$$(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$$

and this happens if and only if the two subgroups $\mathcal{H}_{(\alpha,\beta)}$, $\mathcal{H}_{(\alpha',\beta')}$ of $\mathrm{GL}(\ell, \mathbb{F}_p)$ are conjugate over $\mathrm{GL}(\ell, \mathbb{F}_p)$. In fact, if $\sigma\colon (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \longrightarrow (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$ is an

isomorphism then for every $A \in \mathcal{H}_{(\alpha,\beta)}$ the following diagram must be commutative

$$\begin{array}{ccc} \mathbb{F}_p^\ell & \xrightarrow{A} & \mathbb{F}_p^\ell \\ {\scriptstyle \sigma|_{\mathbb{F}_p^\ell}}\downarrow & & \downarrow{\scriptstyle \sigma|_{\mathbb{F}_p^\ell}} \\ \mathbb{F}_p^\ell & \xrightarrow[\sigma(A)]{} & \mathbb{F}_p^\ell \end{array}$$

where $\sigma|_{\mathbb{F}_p^\ell} \in \mathrm{Aut}(\mathbb{F}_p^\ell)$ and thus can be expressed as an invertible matrix in $\mathrm{GL}(\ell, \mathbb{F}_p)$. To classify the various case depending on the value of $s = r/(r, f_K)$, we must distinguish two different situations: $\ell \mid f_K$ and $\ell \nmid f_K$.

For what will follow it is convenient to introduce the function $\psi(a,b)$ that maps $(a,b) \in \mathbb{N} \times \mathbb{N}$ to the number of elements of order a in the group $C_a \times C_b$. It can be expressed as

$$\psi(a,b) = a \cdot (a,b) \cdot \prod_{\substack{l \text{ prime} \\ l \mid (a,b)}} \left(1 - \frac{1}{l^2}\right) \cdot \prod_{\substack{l \text{ prime} \\ l \mid a \\ l \nmid (a,b)}} \left(1 - \frac{1}{l}\right).$$

Moreover, for every c dividing $p^\ell - 1$, we define the function $\lambda(c,p)$ as

$$\lambda(c,p) = \begin{cases} 1 & \text{if } p \equiv 2, \dots, \ell - 1 \pmod{\ell} \text{ or} \\ & p \equiv 1 \pmod{\ell} \text{ and, } v_\ell(c) = 0 \text{ or } v_\ell(c) = v_\ell(p^\ell - 1) \\ \frac{1}{\ell} & \text{if } p \equiv 1 \pmod{\ell} \text{ and } v_\ell(p-1) < v_\ell(c) < v_\ell(p^\ell - 1) \\ \frac{1}{\ell+1} & \text{if } p \equiv 1 \pmod{\ell} \text{ and } 0 < v_\ell(c) \leq v_\ell(p-1) \end{cases} \tag{2.2}$$

CASE $\ell \mid f_K$.

Theorem 2.2. *Let K be a p-adic field, f_K its inertial degree over $\mathbb{Q}_p$ and $n_K = [K : \mathbb{Q}_p]$. Let ℓ be a prime number and suppose that $\ell \mid f_K$. Then the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields is of type $\mathbb{F}_{p^\ell}^+ \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^\ell}^*$ not contained in $\mathbb{F}_p^*$ with the natural action on $\mathbb{F}_{p^\ell}^+$.*

Moreover, for every integer c dividing $p^\ell - 1$ but not $p-1$, if C is the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ of order c, then there are

$$n(c) = \frac{1}{\ell} \psi(c, p^\ell - 1) \frac{p^{\ell n_K} - 1}{p^\ell - 1}$$

isomorphism classes of p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$.

Proof. Since ℓ is a prime number and $\ell \mid f_K$, from (2.1) we have that the dimension is ℓ if and only if r and w are equal to 1 or ℓ and at least one of the two is equal to ℓ. Moreover for every α and β satisfying this condition, we always have $\dim J_{(\alpha,\beta)} = s = \frac{r}{(r,f_K)} = 1$. It follows that $\mathcal{H}_{(\alpha,\beta)}$ is generated by the diagonal matrices

$$\begin{pmatrix} \alpha & & & \\ & \alpha^p & & \\ & & \ddots & \\ & & & \alpha^{p^{\ell-1}} \end{pmatrix}, \quad \begin{pmatrix} \beta & & & \\ & \beta^p & & \\ & & \ddots & \\ & & & \beta^{p^{\ell-1}} \end{pmatrix}$$

and therefore it is isomorphic to the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ generated by α and β. Therefore the only case in which $(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$ is when $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$ generate groups of the same order.

Note that if α and β generate the cyclic subgroup C of $\mathbb{F}_{p^\ell}^*$ then $(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq \mathbb{F}_{p^\ell}^+ \rtimes C$, where C acts in the natural way on $\mathbb{F}_{p^\ell}^+$.

Let $c \mid p^\ell - 1$ but $c \nmid p - 1$, then the number of pairs (α, β) in $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_{p^\ell}^*$ having order c is equal to $\psi(c, p^\ell - 1)$. Since $s = 1$ for each of them, the number of representations in F^*/F^{*p} defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $(p^{\ell n_K} - 1)/(p^\ell - 1)$. Observe that we need to count together (α, β), (α^p, β^p) ... $(\alpha^{p^{\ell-1}}, \beta^{p^{\ell-1}})$ since they lead to the same representation over $\mathbb{F}_p$, so we must divide by ℓ.

It follows that if C is the cyclic group of order c in $\mathbb{F}_{p^\ell}^*$, the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$ (where C acts naturally on $\mathbb{F}_{p^\ell}^+$) is exactly

$$\frac{1}{\ell}\psi(c, p^\ell - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}.$$

The groups of type $\mathbb{F}_{p^\ell}^+ \rtimes C$ with $C < \mathbb{F}_{p^\ell}^*$ is the only groups that can appear as Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields when $\ell \mid f_K$. □

CASE $\ell \nmid f_K$.

Theorem 2.3. *Let K be a p-adic field, f_K its inertial degree over $\mathbb{Q}_p$ and $n_K = [K : \mathbb{Q}_p]$. Let ℓ be a prime number and suppose that $\ell \nmid f_K$. Then the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields is either of type $\mathbb{F}_{p^\ell}^+ \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^\ell}^*$ not contained in $\mathbb{F}_p^*$ (with the natural action on $\mathbb{F}_{p^\ell}^+$), or of type $(\mathbb{F}_p)^\ell \rtimes \mathcal{H}$, where $\mathcal{H} \subseteq \mathrm{GL}(\ell, \mathbb{F}_p)$ is isomorphic to a non abelian subgroup of $\mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$.*
Moreover,

- *for every integer c dividing $p^\ell - 1$ but not $p - 1$, if C is the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ of order c, then there are*

$$n(c) = \frac{1}{\ell}\psi(c, p^\ell - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}$$

  isomorphism classes of p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$;

- *for every non abelian subgroup $\mathcal{H} \subseteq \mathrm{GL}(\ell, \mathbb{F}_p)$ isomorphic to a subgroup Z of $\mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$, if $C = Z \cap \mathbb{F}_{p^\ell}^*$ has order c then there are*

$$n(\mathcal{H}) = \begin{cases} \lambda(c,p)\psi(c,p-1)\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p-1} & \text{if } C \to Z \text{ splits} \\ \frac{1-\lambda(c,p)}{\ell-1}\psi(c,p-1)\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p-1} & \text{if } C \to Z \text{ does not split} \end{cases}$$

  isomorphism classes of p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $(\mathbb{F}_p)^\ell \rtimes \mathcal{H}$.

Proof. Since $\ell \nmid f_K$ from (2.1), the dimension of a representation of H over $\mathbb{F}_p$ is ℓ when one of r, w is 1 and the other ℓ.
For $r = 1$ and $w = \ell$, i.e. for the pairs α, β with $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$, it turns out again $\dim J_{(\alpha,\beta)} = s = 1$ so, as above, the group $\mathcal{H}_{(\alpha,\beta)}$ acting on the representation is cyclic of order equal to the order of (α, β) in $(\mathbb{F}_p^* \times \mathbb{F}_{p^\ell}^*) \setminus (\mathbb{F}_p^* \times \mathbb{F}_p^*)$ and for each pair (α, β) there are $(p^{\ell n_K} - 1)/(p^\ell - 1)$ representations over $\mathbb{F}_p$ containing a unique copy of $J_{(\alpha,\beta)}$.
Let $c \mid p^\ell - 1$ but $c \nmid p - 1$, the possible pairs (α, β) in $\mathbb{F}_p^* \times \mathbb{F}_{p^\ell}^*$ of order c are $\psi(c, p-1)$. Thus, similarly to above, if C is the cyclic group of order c in $\mathbb{F}_{p^\ell}^*$ then the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$ is

$$\frac{1}{\ell}\psi(c, p^\ell - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}.$$

For $r = \ell$ and $w = 1$ we have $\dim J_{(\alpha,\beta)} = s = \frac{r}{(r,f_K)} = \ell$ and $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$. It follows that the group $\mathcal{H}_{(\alpha,\beta)}$ coincides with the group of matrices which describe the action on $J_{(\alpha,\beta)}$.

Recalling that $q = p^{f_K}$ and $\ell \nmid f_K$, from the study of the representations of H we have made in Section 1.3, we find that the action of H on $J_{(\alpha,\beta)}$ is described by the matrices

$$T_\alpha = \begin{pmatrix} \alpha & & & \\ & \alpha^p & & \\ & & \ddots & \\ & & & \alpha^{p^{\ell-1}} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & & & \beta \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

So $\mathcal{H}_{(\alpha,\beta)} = \langle T_\alpha, V_\beta \rangle$ is a non-abelian group. Moreover the number of representations contained in F^*/F^{*p} isomorphic to $J_{(\alpha,\beta)}$ is exactly $(p^{\ell n_K} - 1)/(p-1)$. This number must be divided by ℓ when one takes into account that the pairs (α, β), (α^p, β) ... $(\alpha^{p^{\ell-1}}, \beta)$ in $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ give the same representation.

It remains to multiply by the number of pairs (α', β') such that $(\mathbb{F}_p^+)^\ell \rtimes \langle T_{\alpha'}, V_{\beta'} \rangle \simeq (\mathbb{F}_p^+)^\ell \rtimes \langle T_\alpha, V_\beta \rangle$. For what we have remarked above, this means that we have to count the number of pairs $(\alpha', \beta') \in \mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ such that $\langle T_{\alpha'}, V_{\beta'} \rangle$ and $\langle T_\alpha, V_\beta \rangle$ are conjugate in $\mathrm{GL}(\ell, \mathbb{F}_p)$ (note that this is equivalent to require that they are conjugate in $\mathrm{GL}(\ell, \mathbb{F}_{p^\ell})$).

It turns out that $\mathcal{H}_{(\alpha,\beta)}$ is conjugate to $\mathcal{H}_{(\alpha',\beta')}$ if only if there exists a matrix $M \in \mathrm{GL}(\ell, \mathbb{F}_p)$ such that $M^{-1}\mathcal{H}_{(\alpha,\beta)}M = \mathcal{H}_{(\alpha',\beta')}$ and diagonal matrices are sent to diagonal matrices.

In fact, the subgroup of the diagonal matrices of $\mathcal{H}_{(\alpha,\beta)}$ is generated by T_α and V_β^ℓ, it is a maximal cyclic subgroup $\langle T_\gamma \rangle$ of $\mathcal{H}_{(\alpha,\beta)}$ of order equal to $\mathrm{o}(\gamma) = \mathrm{lcm}(\mathrm{o}(\alpha), \mathrm{o}(\beta))$ and index ℓ. Suppose that $\mathcal{H}_{(\alpha,\beta)}$ and $\mathcal{H}_{(\alpha',\beta')}$ are conjugate, then the maximal cyclic subgroups of the diagonal matrices have the same order, and in particular they are equal since they are isomorphic to the same subgroup of $\mathbb{F}_{p^\ell}^*$ via the same map. Therefore $\mathcal{H}_{(\alpha,\beta)} = \langle T_\gamma, V_\beta \rangle$ and $\mathcal{H}_{(\alpha',\beta')} = \langle T_\gamma, V_{\beta'} \rangle$.

Now, $\mathcal{H}_{(\alpha,\beta)}$ and $\mathcal{H}_{(\alpha',\beta')}$ have either only one maximal cyclic subgroup, that is the subgroup of the diagonal matrices, or $\ell + 1$ maximal cyclic subgroups (one of which is that of the diagonal matrices). In the first case, there is nothing to prove since clearly all the conjugations send diagonal matrices in diagonal matrices. For the second case, observe that by the proof of Theorem 2.1, $\mathcal{H}_{(\alpha,\beta)}$ is isomorphic to

$\langle(\gamma,\mathrm{id}),(\gamma,\phi_p)\rangle \subseteq \mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$, i.e. it is isomorphic to a subgroup of the normalizer of a Cartan subgroup of $\mathrm{GL}(\ell,\mathbb{F}_p)$.

The key point is to observe that there always exists a basis under which (γ,id) and (γ,ϕ_p) are represented by the generators of any two cyclic subgroups of index ℓ of $\mathcal{H}_{(\alpha,\beta)}$ and every pairs of these matrices generate the whole group $\mathcal{H}_{(\alpha,\beta)}$. This is enough to prove that we can suppose not only $\langle T_\gamma\rangle$ is sent to $\langle T_\gamma\rangle$ but also that $\langle T_{\alpha^\ell}, V_\beta\rangle$ goes in $\langle T_{\alpha'^\ell}, V_{\beta'}\rangle$.

Therefore there exists a diagonal matrix $D = T_\alpha^i V_\beta^{\ell j} \in \mathcal{H}_{(\alpha,\beta)}$ such that

$$M^{-1}(DV_\beta)M = V_{\beta'}.$$

This leads to

$$\beta' = \gamma^{k(p^{\ell-1}+\cdots+p+1)}\beta,$$

for some $k \in \mathbb{Z}$ and where $\gamma \in \mathbb{F}_{p^\ell}^*$ has order $\mathrm{lcm}(\mathrm{o}(\alpha),\mathrm{o}(\beta)) = \mathrm{lcm}(\mathrm{o}(\alpha'),\mathrm{o}(\beta'))$.

Consequently the Galois group is identified by the order of the cyclic group $C = \langle\gamma\rangle \subseteq \mathbb{F}_{p^\ell}^*$ and the class of β in $(C\cap\mathbb{F}_p^*)/C^{p^{\ell-1}+\cdots+p+1}$.

Let c be the order of C. Since

$$(p-1, p^{\ell-1}+\cdots+p+1) = \begin{cases} \ell & \text{if } p \equiv 1 \pmod{\ell} \\ 1 & \text{if } p \equiv 2,\ldots,\ell-1 \pmod{\ell} \text{ or } p = \ell \end{cases}$$

we have

$$\left|\frac{C\cap\mathbb{F}_p^*}{C^{p^{\ell-1}+\cdots+p+1}}\right| = \begin{cases} \ell & \text{if } p \equiv 1 \pmod{\ell} \text{ and } 0 < v_\ell(c) < v_\ell(p^\ell-1) \\ 1 & \text{otherwise.} \end{cases}$$

Clearly, if $|(C\cap\mathbb{F}_p^*)/C^{p^{\ell-1}+\cdots+p+1}| = 1$ then there is only one class mod $C^{p^{\ell-1}+\cdots+p+1}$, therefore every pairs (α,β) such that α and β generate C give (class of) extensions with isomorphic Galois groups.

We now consider the case $|(C\cap\mathbb{F}_p^*)/C^{p^{\ell-1}+\cdots+p+1}| = \ell$.

Suppose $\ell^k \parallel c$, then $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if and only if its order is not divisible by a power of ℓ greater than $\ell^k/(\ell^k, p^{\ell-1}+\cdots+p+1)$.

On the other hand, we have that $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if and only if the map $C \hookrightarrow \langle T_\alpha, V_\beta\rangle$ splits (abusing notation, we have identified C with its image in $\langle T_\alpha, V_\beta\rangle$). In fact, this map splits if and only if β has an ℓ-root in C, i.e. there exists $t \in C$ such that $t^\ell = \beta$. This is equivalent to say that there exists $r \in C$ such that

$r^{p^{\ell-1}+\cdots+p+1} = \beta$ since $C^{p^{\ell-1}+\cdots+p+1} = (C \cap \mathbb{F}_p^*)^{p^{\ell-1}+\cdots+p+1} = (C \cap \mathbb{F}_p^*)^{\ell}$.

We write $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ as direct sum of l-groups for each prime l, and chose the components of (α, β) in this sum among the elements of the correct order. For what we have said above, for $l \neq \ell$ the choice of the l-component of (α, β) has no effect on the condition $\beta \in C^{p^{\ell-1}+\cdots+p+1}$.

For $l = \ell$, if C_n denotes the cyclic group of order n, the ℓ-part of $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ is $C_{\ell^{m+z}} \times C_{\ell^z}$ where $\ell^m \parallel p^{\ell-1}+\cdots+p+1$ and $\ell^z \parallel p-1$. Recall that $\ell^k \parallel c$ for some $1 \leq k < m+z$. Since we are considering the case $(p-1, p^{\ell-1} + \cdots + p + 1) = \ell$, we have $z = 1$ or $m = 1$.

If $z = 1$ then the ℓ-part of $C^{p^{\ell-1}+\cdots+p+1}$ is trivial, therefore $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ when the ℓ-component of (α, β) is of type $(x, 1)$, and this happens for $\frac{\phi(\ell^k)}{\ell\phi(\ell^k)} = \frac{1}{\ell}$ of the possible ℓ-components when $k > 1$ and for $\frac{\ell-1}{\ell^2-1} = \frac{1}{\ell+1}$ of the possible ℓ-components when $k = 1$.

If $m = 1$ then $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if its order is not divisible by a power of ℓ greater than ℓ^{k-1}, therefore the ℓ-component of (α, β) must be of type (x, y) with the order of x greater than the order of y; this is true for $\frac{\phi(\ell^k)\ell^{k-1}}{2\phi(\ell^k)\ell^k - \phi(\ell^k)^2} = \frac{1}{\ell+1}$ of the elements with correct order.

Recollecting all the informations achieved, we have that if λ is the function defined in (2.2), then $\lambda(c,p)\psi(c,p-1)$ is the number of pairs (α, β) such that the group C generated by α and β has order c and $\beta \in C^{p^{\ell-1}+\cdots+p+1}$, while $(1-\lambda(c,p))\psi(c,p-1)$ counts the same pairs but with $\beta \notin C^{p^{\ell-1}+\cdots+p+1}$.

Finally, to conclude the proof, it remains to observe that the β's not contained in $C^{p^{\ell-1}+\cdots+p+1}$ are equally distributed in each of the $\ell - 1$ non trivial classes modulo $C^{p^{\ell-1}+\cdots+p+1}$. □

2.4 Ramification groups and Discriminant

We know that there is a one-to-one correspondence between the isomorphism classes of extensions of degree p^ℓ of K having no intermediate extensions and the irreducible H-submodules of dimension ℓ of F^*/F^{*p}, or equivalently, the abelian p^ℓ-extensions of F of exponent p, Galois over K, having no intermediate subextensions that are Galois over K.

Denote by $\mathscr{C}_{p^\ell}$ the composite of all extensions of degree p^ℓ of K having no intermediate fields. Clearly $\mathscr{C}_{p^\ell}/K$ is Galois. We want to determine the ramification groups

of its Galois group.
Let $\mathscr{G} = \mathrm{Gal}(\mathscr{C}_{p^\ell}/K)$. As usual for $i \geq -1$ we denote by $\mathscr{G}_i$ the i-th ramification group of $\mathscr{G}$.

Lemma 2.4. *One has*

$$\mathscr{C}_{p^\ell} = \mathscr{A}_F^{(p^\ell)}$$

where $\mathscr{A}_F^{(p^\ell)}$ is the composite of all abelian p^ℓ-extensions of F of exponent p having no other subextensions that are Galois over K.

Proof. If L/K is a p^ℓ-extension having no intermediate fields, then LF is contained in $\mathscr{A}_F^{(p^\ell)}$ (see proof of Theorem 2.1), therefore $\mathscr{C}_{p^\ell} \subseteq \mathscr{A}_F^{(p^\ell)}$.
Conversely, let E be an abelian p^ℓ-extension of F of exponent p, Galois over K having no subextensions that are Galois over K. As seen in the proof of Theorem 2.1, $\mathrm{Gal}(E/K) \simeq \Xi \rtimes H$ where Ξ is the $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} of dimension ℓ which corresponds to E/F by Kummer theory, E^H is an extension of K of degree p^ℓ having no intermediate fields, so that $E^H \subseteq \mathscr{C}_{p^\ell}$, and $E^H F = E$.
Since $E^H \subseteq \mathscr{C}_{p^\ell}$, the Galois closure of E^H over K is also contained in $\mathscr{C}_{p^\ell}$ ($\mathscr{C}_{p^\ell}/K$ being Galois) and it is the composite of E^H with a suitable subextension of F/K (see proof of Theorem 2.1), which is then contained in $\mathscr{C}_{p^\ell}$. By the definition of F, as E varies through the elements of $\mathscr{A}_F^{(p^\ell)}$ with E/K Galois, these subextensions generate F, so that $F \subseteq \mathscr{C}_{p^\ell}$ and hence $E \subseteq \mathscr{C}_{p^\ell}$. In fact F is the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}_{p^\ell}^*$ or to a non abelian subgroup of $\mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ and for each of these subextensions, by Theorem 2.2 and 2.3, there exists $E \subseteq \mathscr{A}_F^{(p^\ell)}$ such that the Galois closure of E^H over K contains this subfield of F.
Finally observe that these extensions E are sufficient to generate $\mathscr{A}_F^{(p^\ell)}$, thus we have $\mathscr{A}_F^{(p^\ell)} \subseteq \mathscr{C}_{p^\ell}$. □

Lemma 2.4 implies that $\mathscr{C}_{p^\ell}/F$ is a subextension of $\mathscr{A}_F/F$, where $\mathscr{A}_F$ is the maximal abelian extension of F of exponent p. Thus $[\mathscr{C}_{p^\ell} : F] = p^t$ for some $t \leq n_F + 2$ (see [DCD07, Prop 3]). By Kummer theory, we know that $\mathscr{C}_{p^\ell}$ corresponds to a subgroup of F^*/F^{*p} and $[\mathscr{C}_{p^\ell} : F]$ is equal to the order of this subgroup (clearly F contains the p-th roots of 1).

Proposition 2.5. *One has*

$$[\mathscr{C}_{p^\ell} : F] = \begin{cases} p^{((p^\ell-1)^2-(p-1)^2)n_K} & \text{if } \ell \mid f_K \\ p^{(\ell+1)(p^\ell-p)(p-1)n_K} & \text{if } \ell \nmid f_K \end{cases}.$$

Proof. By Lemma 2.4, $[\mathscr{C}_{p^\ell} : F] = [\mathscr{A}_F^{(p^\ell)} : F]$ and $\mathscr{A}_F^{(p^\ell)} = F(\sqrt[p]{\Delta})$, where Δ is the $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} generated by the irreducible submodules of dimension ℓ. It follows that $[\mathscr{C}_{p^\ell} : F]$ is the order of Δ.

Δ can be generated by a finite number of disjoint irreducible $\mathbb{F}_p[H]$-submodules of dimension ℓ; clearly if m is their number then $[\mathscr{C}_{p^\ell} : F] = p^{\ell m}$.

By (1.3), we know that

$$F^*/F^{*p} \simeq \mathbb{F}_p \oplus \bigoplus_{i \in [\![0, I_F]\!]} M_i \oplus M_\omega$$

as $\mathbb{F}_p[H]$-modules; the $\mathbb{F}_p[H]$-modules of dimension ℓ are contained in $\bigoplus_{i\in[\![0,I_F]\!]} M_i$. Moreover, we know that such a module V is the sum of the conjugates of a certain $J_{(\alpha,\beta)}$, which is an $\overline{\mathbb{F}}_p[H]$-submodule of $\overline{M}_i = M_i \oplus_{\mathbb{F}_p} \overline{\mathbb{F}}_p$; as α and β vary in $\mathbb{F}_{p^\ell}^*$ we find all the irreducible representations of dimension ℓ contained in F^*/F^{*p}. The multiplicity of V in $\bigoplus_{i\in[\![0,I_F]\!]} M_i$ is equal to that of $J_{(\alpha,\beta)}$ in $Y = \bigoplus_{i\in[\![0,I_F]\!]} \overline{M}_i$: it counts the number of disjoint $\mathbb{F}_p$-vector space (respectively $\overline{\mathbb{F}}_p$-vector space) in F/F^{*p} on which H acts as on V (respectively $J_{(\alpha,\beta)}$).

In particular, by equation (2.1), if $\ell \mid f_K$ then to achieve $\mathbb{F}_p$-representations of dimension ℓ we must have $(\alpha, \beta) \in (\mathbb{F}_{p^\ell}^* \times \mathbb{F}_{p^\ell}^*) \setminus (\mathbb{F}_p^* \times \mathbb{F}_p^*)$ and, for each of these pairs, $J_{(\alpha,\beta)}$ has dimension 1 and multiplicity n_K. As usual observe that the $\mathbb{F}_p$-representation containing $J_{(\alpha,\beta)}$ is equal to that containing its other $\ell-1$ conjugates, that is $J_{(\alpha^p,\beta^p)}, \ldots, J_{(\alpha^{p^{\ell-1}},\beta^{p^{\ell-1}})}$. Therefore we have

$$m = \frac{1}{\ell}[(p^\ell - 1)^2 - (p-1)^2]n_K.$$

If $\ell \nmid f_K$, then only one between α and β is in $\mathbb{F}_{p^\ell}^* \setminus \mathbb{F}_p^*$ and the other in $\mathbb{F}_p^*$. The $J_{(\alpha,\beta)}$'s with $\alpha \in \mathbb{F}_{p^\ell}^*$ and $\beta \in \mathbb{F}_p^*$ have no conjugates different from itself and multiplicity ℓn_K, but $J_{(\alpha,\beta)} = J_{(\alpha^p,\beta)} = \cdots = J_{(\alpha^{p^{\ell-1}},\beta)}$; while the $J_{(\alpha,\beta)}$'s with $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$ have multiplicity n_K and ℓ conjugates like the previous case. Thus we have

$$m = (p^\ell - p)(p-1)n_K + \frac{1}{\ell}(p-1)(p^\ell - p)n_K.$$

Substituting in $[\mathscr{C}_{p^\ell} : F] = p^{\ell m}$, we obtain the thesis. □

Observe that, by the Theorem 2.1, $\mathscr{G} \simeq G \rtimes H$, where G is the Galois group of $\mathscr{C}_{p^\ell}$ over F. It is well known that $\mathscr{G}_{-1} = \mathscr{G}$, $\mathscr{G}_0$ is the inertia subgroup of $\mathscr{G}$ and $\mathscr{G}_1$ is the p-Sylow subgroup of $\mathscr{G}_0$. By the proof of Proposition 2.5 we have that $\mathscr{C}_{p^\ell}/F$ is a totally ramified extension; in fact $\mathscr{C}_{p^\ell} = F(\sqrt[p]{\Delta})$ where Δ is contained in $\bigoplus_{i\in[\![0,I_F]\!]} M_i$ which is disjoint from M_ω that corresponds to the unramified extension of F of degree p ($\mathscr{C}_{p^\ell}/F$ can contain no other unramified subextension since it is elementary abelian and therefore its cyclic subextensions are of degree p). It follows that $\mathscr{G}_0$ is isomorphic to $G \rtimes H_0$ where H_0 is the inertia subgroup of H, while $\mathscr{G}_i \simeq G_i$ for all $i \geq 1$ since F/K is tame.

It is suitable to search the upper numbering ramification groups because, if L is a Galois extension of F contained in $\mathscr{C}_{p^\ell}$ and $G_L = \mathrm{Gal}(\mathscr{C}_{p^\ell}/L)$ then for all v one has $(G/G_L)^v \simeq G^v G_L/G_L$ (see [Ser79], Ch. IV, §3, Prop. 14) and, in our case, if also L has degree p^ℓ over F and is Galois over K, then the groups $(G/G_L)^v$ are easy to describe.

Lemma 2.6. *Let*

$$d = \begin{cases} ((p^\ell-1)^2 - (p-1)^2)n_K & \text{if } \ell \mid f_K \\ (\ell+1)(p^\ell - p)(p-1)n_K & \text{if } \ell \nmid f_K \end{cases}.$$

One has

$$\dim_{\mathbb{F}_p} G^v = \begin{cases} d & \text{if } -1 \leq v \leq 1 \\ d - \left(\lceil v \rceil - \left\lceil \frac{v}{p} \right\rceil\right) f_F & \text{if } 1 < v \leq \frac{pe_F}{p-1} - 1 \\ 0 & \text{if } v > \frac{pe_F}{p-1} - 1 \end{cases}.$$

Proof. First of all observe that $\mathscr{C}_{p^\ell}/F$ is a totally and wildly ramified extension, therefore $G_{-1} = G_0 = G_1 = G$; moreover a simple calculation of the Herbrand's function (see [Ser79], Ch. IV, §3) yields to $G^1 = G_1$ so that for $-1 \leq v \leq 1$ one has $G^v = G = \mathrm{Gal}(\mathscr{C}_{p^\ell}/F)$ and $\dim_{\mathbb{F}_p} G^v = d$. Moreover, since $\mathscr{C}_{p^\ell}/F$ is an elementary abelian p-extension, by Theorem 12 of [CDC15], for every $v > pe_F/(p-1)$ we have $G^v = 1$, i.e. $\dim_{\mathbb{F}_p} G^v = 0$. It remains to determine $\dim_{\mathbb{F}_p} G^v$ when $1 < v \leq pe_F/(p-1)$.

Let L be an abelian p^ℓ-extension of F of exponent p having no subextensions that are Galois over K and let $G_L = \mathrm{Gal}(\mathscr{C}_{p^\ell}/L)$.

As remarked before, we know that for all v one has $(G/G_L)^v \simeq G^v G_L/G_L$, hence

$$G^v = \bigcap_{(G/G_L)^v=1} G_L.$$

Via Galois theory, this group corresponds to $\mathscr{C}_{p^\ell}^{G^v} = \prod L$, with the composite taken over the abelian p^ℓ-extensions L/F satisfying the previous condition, i.e. such that $(G/G_L)^v = 1$. It follows that $\dim_{\mathbb{F}_p} G^v$ is equal to d minus the dimension of the $\mathbb{F}_p$-vector space associated to $\prod L$ by Kummer theory.
Since $G/G_L \simeq \mathrm{Gal}(L/F) \simeq (\mathbb{Z}/p\mathbb{Z})^\ell$, by Proposition 7 in [CDC15] L/F has an upper ramification jump in t if and only if there exists a subextension N/F of degree p with upper ramification jump equal to t; moreover the jumps can only appear in the integers t such that $1 \leq t \leq pe_F/(p-1)$ and $(t,p) = 1$. Therefore, for all $v > pe_F/(p-1)$, $(G/G_L)^v = 1$ for every abelian p^ℓ-extension L/F.
Let v be a real number such that $1 < v \leq pe_F/(p-1)$, then $G^v = G^{\lceil v \rceil}$ and $G^{\lceil v \rceil}$ is the subgroup of G fixing the composite of all the abelian p^ℓ-extensions L/F which have a jump in $\mathcal{J} = \{1, \ldots, \lceil v \rceil - 1\}$. Using Proposition 14 of [CDC15] and the analysis of the possible representation associated to L we have made in section 1.3, we find that there are f_F disjoint extensions L/F which have a jump in a fixed $t \in \mathcal{J}$ and $(t,p) = 1$. Since the possible t's are $\lceil v \rceil - \left\lceil \frac{v}{p} \right\rceil$, we have the thesis. □

Note that our result is in agreement with Lemma 9 of [DCD07].
We can now prove the following

Proposition 2.7. *Let d be as in previous Lemma 2.6. The ramification groups $\mathscr{G}_i$ of $\mathscr{C}_{p^\ell}/K$ are:*

$$\begin{aligned}
\mathscr{G}_{-1} &= \mathscr{G} = G \rtimes H, \\
\mathscr{G}_0 &= G \rtimes H_0, \\
\mathscr{G}_i &= (\mathbb{Z}/p\mathbb{Z})^{d-kf_F} && \text{if } t(k-1) < i \leq t(k), \\
\mathscr{G}_i &= \{e\} && \text{if } i > t(e_F - 1),
\end{aligned}$$

where $t(-1) = 0$, $t(0) = 1$ and for every $1 \leq k \leq e_F - 1$,

$$t(k) = \begin{cases} t(k-1) + p^{kf_F} & \text{if } k \not\equiv 0 \pmod{p-1} \\ t(k-1) + 2p^{kf_F} & \text{if } k \equiv 0 \pmod{p-1}. \end{cases}$$

Therefore there are $e_F + 2$ jumps in the lower ramification groups.

Proof. The claim for $\mathscr{G}_{-1}$ and $\mathscr{G}_0$ is clear by the considerations we have made before, $\mathscr{G}_1 = G_1$ since $\mathscr{C}_{p^\ell}/F$ is wildly ramified and so F/K is the maximal tame subextension. The rest of the Proposition follows by Lemma 2.6 with simple calculations, recalling that $\mathscr{G}_i = G_i$ for all $i \geq 1$ and the Herbrand's function (see [Ser79], Ch. IV, §3)

$$G^v = G_{\psi(v)} \quad \text{with} \quad \psi(v) = \int_0^v (G^0 : G^w)dw$$

which relates the upper and the lower ramification filtrations.
Lemma 2.6 says that G has jumps in the upper ramification in every integers of $[\![0, \frac{pe_F}{p-1}]\!]$, i.e. in the integers of the set $\{1 \leq v \leq \frac{pe_F}{p-1} - 1 \mid v \not\equiv 0 \pmod{p}\}$; every such jump of G gives a jump in the lower ramification of $\mathscr{G}$, and these together with -1 and 0 are exactly the $e_F + 2$ jumps of $\mathscr{G}$. □

Finally we determine the discriminant $\mathfrak{d}_{\mathscr{C}_{p^\ell}/K}$ of $\mathscr{C}_{p^\ell}/K$.

Proposition 2.8. *If π_K is a uniformizer of K and $d = [\mathscr{C}_{p^\ell} : F]$ as in the previous Lemma 2.6 then*

$$\mathfrak{d}_{\mathscr{C}_{p^\ell}/K} = (\pi_K)^\alpha$$

where

$$\alpha = f_{F/K}\left(\left([F:K] - 1 + \frac{p(e_F+1)-1}{p-1}\right)p^d - 1 - \frac{p^{n_F}-1}{p^{f_F}-1} - \frac{p^{n_F}-1}{p^{(p-1)f_F}-1}\right).$$

Proof. Using the well known formula

$$v_{\mathscr{C}_{p^\ell}}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}) = \sum_{i=0}^{\infty}(|\mathscr{G}_i| - 1)$$

where $\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}$ is the different of $\mathscr{C}_{p^\ell}/K$, one gets

$$v_{\mathscr{C}_{p^\ell}}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}) = [F:K]p^d - 1 + \sum_{k=0}^{e_F-1}(p^{d-kf_F} - 1)p^{kf_F} +$$
$$+ \sum_{\substack{k=1 \\ k\equiv 0 \pmod{p-1}}}^{e_F-1}(p^{d-kf_F} - 1)p^{kf_F}.$$

The conclusion follows by a simple calculation, recalling that

$$\mathfrak{d}_{\mathscr{C}_{p^\ell}/K} = N_{\mathscr{C}_{p^\ell}/K}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K})$$

where $N_{\mathscr{C}_{p^\ell}/K}$ is the norm map and observing that, since $\mathscr{C}_{p^\ell}/F$ is totally ramified, $N_{\mathscr{C}_{p^\ell}/K}(\pi_{\mathscr{C}_{p^\ell}}) = (\pi_K)^{f_{F/K}}$ ($\pi_{\mathscr{C}_{p^\ell}}$ is a uniformizer of $\mathscr{C}_{p^\ell}$). □

2.5 The field F when $\ell = 2$

We determine an explicit description of F in the case $\ell = 2$.
Let F be the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}_{p^2}^*$ or to a non-abelian subgroup of $\mathbb{F}_{p^2}^* \rtimes_\theta \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ where $\theta(\phi_p) = \phi_{p|\mathbb{F}_{p^2}^*} \in \mathrm{Aut}(\mathbb{F}_{p^2}^*)$ (ϕ_p the Frobenius automorphism), and let $H = \mathrm{Gal}(F/K)$ (note that if $p \neq 2$ the hypothesis about the degree is redundant). Denote by ζ_n a primitive n-th root of unity, then the following holds

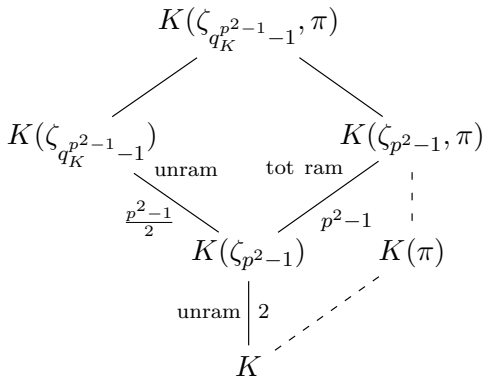
Proposition 2.9. *If $p \neq 2$ or, $p = 2$ and $2 \mid f_K$, one has $F = K(\zeta_{q_K^{p^2-1}-1}, \pi)$ where $\pi^{p^2-1} = \pi_K$, $[F : K] = (p^2-1)^2$ and*

$$H \simeq \begin{cases} \mathbb{Z}/(p^2-1)\mathbb{Z} \times \mathbb{Z}/(p^2-1)\mathbb{Z} & \text{if } 2 \mid f_K \\ \left(\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z} \times \mathbb{Z}/(p^2-1)\mathbb{Z}\right) \rtimes \mathbb{Z}/2\mathbb{Z} & \text{if } 2 \nmid f_K \end{cases}$$

where, in the case $2 \nmid f_K$, the non-zero element of $\mathbb{Z}/2\mathbb{Z}$ acts trivially on $\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ and as multiplication by p on $\mathbb{Z}/(p^2-1)\mathbb{Z}$.
If $p = 2$ and $2 \nmid f_K$, one has $F = K(\zeta_{q_K^3-1})$, $[F : K] = 3$ and $H \simeq \mathbb{Z}/3\mathbb{Z}$.

Proof. The case $p = 2$ and $2 \nmid f_K$ is simple because $\mathbb{F}_4^* \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \simeq S_3$ has only one subgroup of odd order, that is the cyclic group of order 3, and since $\zeta_3 \notin K$ there is only one normal extension of degree 3 of K, that is the unique unramified one. The claim about the Galois group is then trivial.
To prove the remaining part of the proposition it is useful to distinguish two cases: $2 \mid f_K$ and, $2 \nmid f_K$ and $p \neq 2$.
If $2 \mid f_K$ then K contains the (p^2-1)-th roots of unity. Therefore the unramified extension $K(\zeta_{q_K^{p^2-1}-1})/K$ and the totally ramified extension $K(\pi)/K$ are both cyclic of order p^2-1, so that $K(\zeta_{q_K^{p^2-1}-1}, \pi) \subseteq F$. We must show the inverse inclusion. Let L/K be a normal extension with Galois group isomorphic to a subgroup of $\mathbb{F}_{p^2}^*$ or to a non-abelian subgroup of $\mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, and let e and f be its ramification index and inertial degree respectively. By basic theory, $L = K(\zeta_{q_K^f-1}, \pi_L)$ where π_L is a root of the polynomial $X^e - u\pi_K$, for some root of unity u in $K(\zeta_{q_K^f-1})$. The thesis follows if we show that $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and that u is a e-th power in $K(\zeta_{q_K^{p^2-1}-1})$, i.e. $K(\zeta_{q_K^{p^2-1}-1})$ contains the $e(q_K^f-1)$-th roots of unity. This last statement is equivalent to show that $e(q_K^f-1) \mid q_K^{p^2-1}-1$. If L/K is cyclic then $ef \mid p^2-1$,

and in particular $e \mid p^2-1$ and $f \mid p^2-1$ therefore $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$. Moreover $q_K^{p^2-1}-1 = q_K^{eft}-1 = (q_K^f-1)((q_K^f)^{et-1}+\cdots+1)$ and the factor at the right is the sum of et addends, each of which is congruent to 1 modulo e because $q_K \equiv 1 (\mathrm{mod}\ e)$ since $2 \mid f_K$ and $p^2 \equiv 1 (\mathrm{mod}\ e)$. So we have proved that $L \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. Now we show that if $2 \mid f_K$ then there exists no extension L/K such that $\mathrm{Gal}(L/K) \simeq D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with $D < \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$, thus proving that $F \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. If $p = 2$, then this is trivial since $\mathbb{F}_4^* \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \simeq S_3$ has no non-cyclic subgroup of odd order. If $p \neq 2$, it suffices to observe that every quotient $\mathrm{Gal}(L/K)/G_0$ acts trivially on the inertia subgroup G_0. This is true because one can easily see that, since $D \not\subseteq \mathbb{F}_p^*$, the only normal and cyclic subgroups of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ are the subgroups of $D \subseteq \mathbb{F}_{p^2}^*$, therefore G_0 can be embedded in $\mathbb{F}_{p^2}^*$ and the Frobenius $\phi_{q_K} = \phi_{p^{f_K}}$ acts trivially on it since f_K is even.
Thus $F = K(\zeta_{q_K^{p^2-1}-1}, \pi)$ and, since the extensions $K(\zeta_{q_K^{p^2-1}-1})/K$ and $K(\pi)/K$ are linearly disjoint, we have $[F:K] = (p^2-1)^2$ and $H \simeq (\mathbb{Z}/(p^2-1)\mathbb{Z})^2$.
If $2 \nmid f_K$ and $p \neq 2$, then K does not contain the (p^2-1)-th roots of unity. The unramified extension $K(\zeta_{q_K^{p^2-1}-1})/K$ is again cyclic of order p^2-1, while the totally ramified extension $K(\pi)/K$ is not cyclic (it is not even Galois). Nevertheless $K(\zeta_{q_K^{p^2-1}-1}, \pi)/K$ is the composite of $K(\zeta_{q_K^{p^2-1}-1})/K$ with the normal extension $K(\zeta_{p^2-1}, \pi)$, and this last is of the type asked because $\mathrm{Gal}(K(\zeta_{p^2-1}, \pi)/K) \simeq \mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$.



So again $K(\zeta_{q_K^{p^2-1}-1}, \pi) \subseteq F$. It remains to prove the inverse inclusion. Let L/K be a normal extension with $\mathrm{Gal}(L/K)$ isomorphic to a subgroup of $\mathbb{F}_{p^2}^*$ or to a non-abelian subgroup of $\mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, e and f its ramification index and inertial degree respectively. As usual we can write $L = K(\zeta_{q_K^f-1}, \pi_L)$ where π_L is a root of the polynomial $X^e - u\pi_K$, for some root of unity u in $K(\zeta_{q_K^f-1})$, thus we must show

that $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and that $K(\zeta_{q_K^{p^2-1}-1})$ contains the $e(q_K^f-1)$-th roots of unity. If L/K is cyclic then $ef \mid p^2-1$, therefore $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and, like the previous case, $q_K^{p^2-1}-1 = q_K^{eft}-1 = (q_K^f-1)((q_K^f)^{et-1}+\cdots+1)$ with the factor at the right divisible by e since it is the sum of et addends, each of which is congruent to 1 modulo e because $q_K^f \equiv 1 (\mathrm{mod}\, e)$ since $L/K(\zeta_{q_K^f-1})$ is cyclic and thus $K(\zeta_{q_K^f-1})$ contains the e-th roots of unity. So $L \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. Suppose now that $\mathrm{Gal}(L/K) \simeq D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with $D < \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$. Since the only normal and cyclic subgroup of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ are those of D, the inertia subgroup G_0 is contained in $D \subseteq \mathbb{F}_{p^2}^*$ so $|G_0| = e \mid p^2-1$; moreover $\mathrm{Gal}(L/K)/G_0$ is a cyclic group of order f, therefore it is contained in the largest abelian quotient of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ whose order, as one can easily see, divides p^2-1. It follows that necessarily $f \mid p^2-1$ and thus $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$. From $e \mid p^2-1$ we also have $2 \mid f$; it follows that $K(\zeta_{q_K^f-1})$ (and hence L) contains the cyclic subextension $K(\zeta_{p^2-1})/K$ of order 2 and $\mathrm{Gal}(K(\zeta_{q_K^f-1}, \pi_L)/K(\zeta_{p^2-1})) \simeq D$, therefore by the previous case $K(\zeta_{q_K^f-1}, \pi_L)$ is contained in $K(\zeta_{q_K^{p^2-1}-1}, \pi)$. This concludes the proof that $F \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$.
Finally, observe that F is the composite of the Galois extensions $K(\zeta_{q_K^{p^2-1}-1})/K$ and $K(\zeta_{p^2-1}, \pi)/K$, and that $K(\zeta_{q_K^{p^2-1}-1}) \cap K(\zeta_{p^2-1}, \pi) = K(\zeta_{p^2-1})$. We have that $K(\zeta_{q_K^{p^2-1}-1})/K(\zeta_{p^2-1})$ is cyclic of order $\frac{p^2-1}{2}$ and $K(\zeta_{p^2-1}, \pi)/K(\zeta_{p^2-1})$ is cyclic of order p^2-1, thus $[F : K] = \frac{p^2-1}{2}(p^2-1)2 = (p^2-1)^2$ and $\mathrm{Gal}(F/K) \simeq \left(\mathrm{Gal}(\mathbb{F}_{q_K^{p^2-1}}/\mathbb{F}_{q_K^2}) \times \mathbb{F}_{p^2}^*\right) \rtimes \mathrm{Gal}(\mathbb{F}_{q_K^2}/\mathbb{F}_{q_K})$; taking into account that $2 \nmid f_K$ it is easy to see that this group is isomorphic to that in the claim. □

Chapter 3

Extensions of degree p^4

We now apply the correspondence Theorem 1.8 to determine the number of isomorphism classes of extensions of degree p^4 of K having no intermediate extensions, and to identify the Galois group of their normal closure. As outlined in the Introduction, we will see that this task is more laborious than that of the previous chapter, in which we had extensions of degree p^ℓ with ℓ a prime number and so representations of dimension a prime. The presence of a further divisor in the required dimension of the representations gives rise to a relevant increase of the number of cases to deal with.

In this chapter, F will be the composite of all normal and tame extensions of K whose Galois group is a subgroup of $\mathrm{GL}(4,\mathbb{F}_p)$, and H will be its Galois group over K.

By equation (1.1), to study the extensions of degree p^4 of K having no intermediate fields, we have to force

$$\dim_{\mathbb{F}_p} V = \mathrm{lcm}\left(\frac{rw}{(r, f_K)}, r\right) = 4. \tag{3.1}$$

which implies r and w equal to 1, 2 or 4.

Analogously to the case of p^ℓ-extensions, if L/K is a p^4-extension having no intermediate fields and $\tilde{L}$ is its normal closure then, by Theorem 1.8,

$$\mathrm{Gal}(\tilde{L}/K) \simeq V \rtimes_{\bar{\rho}} \bar{H}$$

where $\bar{\rho}$ is the map induced on the quotient $\bar{H} = H/\ker\rho$ and the pair (V, ρ) is the representation of dimension 4 of H in F^*/F^{*p}, which corresponds to the class of

L/K under the correspondence of Theorem 1.8. In other words, $\mathrm{Gal}(\tilde{L}/K)$ is the semidirect product of V with the largest quotient of H acting faithfully on it.
Fixing a basis of the $\mathbb{F}_p$-vector space V, we can identify the image of ρ with a subgroup of $\mathrm{GL}(4, \mathbb{F}_p)$, so that $\mathrm{Gal}(\tilde{L}/K) \simeq (\mathbb{F}_p^+)^4 \rtimes \mathcal{H}_\rho$ where $\mathcal{H}_\rho$ represents the action of $\bar{H}$ on V given by $\bar{\rho}$, expressed with respect to the fixed basis.
The normal closures of two isomorphism classes have the same Galois group if and only if

$$(\mathbb{F}_p^+)^4 \rtimes \mathcal{H}_\rho \simeq (\mathbb{F}_p^+)^4 \rtimes \mathcal{H}_{\rho'}$$

and this happens if and only if the two subgroups $\mathcal{H}_\rho$, $\mathcal{H}_{\rho'}$ of $\mathrm{GL}(4, \mathbb{F}_p)$ are conjugate over $\mathrm{GL}(4, \mathbb{F}_p)$.

For what will follow it is convenient to recall the function $\psi(a, b)$ introduced in Section 2.3: it maps $(a, b) \in \mathbb{N} \times \mathbb{N}$ to the number of elements of order a in the group $C_a \times C_b$ and can be expressed as

$$\psi(a,b) = a \cdot (a,b) \cdot \prod_{\substack{l \text{ prime} \\ l \mid (a,b)}} \left(1 - \frac{1}{l^2}\right) \cdot \prod_{\substack{l \text{ prime} \\ l \mid a \\ l \nmid (a,b)}} \left(1 - \frac{1}{l}\right).$$

By equation (3.1), we must distinguish two cases: $4 \mid f_K$ and $4 \nmid f_K$.

3.1 The total number of isomorphism classes and Galois groups when $4 \mid f_K$

Theorem 3.1. *Let K be a p-adic field, f_K be its inertial degree over $\mathbb{Q}_p$ and $n_K = [K : \mathbb{Q}_p]$; suppose that $4 \mid f_K$. Then there are*

$$\frac{1}{4} \frac{p^{4n_K} - 1}{p^4 - 1} (p^8 - 3p^4 + 2p^2)$$

isomorphism classes of extensions of degree p^4 of K having no intermediate fields. Moreover the groups that can appear as Galois group of the normal closure of these extensions are exactly those isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$ where C is a subgroup of $\mathbb{F}_{p^4}^*$ not contained in $\mathbb{F}_{p^2}^*$ (with the natural action on $\mathbb{F}_{p^4}^+$). In particular, for every c dividing

p^4-1 but not p^2-1, if C is the subgroup of $\mathbb{F}_{p^4}^*$ of order c, then there are

$$n(c) = \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}\psi(c, p^4-1)$$

isomorphism classes of p^4-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$.

Proof. By equation (3.1), since $4 \mid f_K$, we have the following possibilities

- $r = 4$ and $w = 1, 2, 4$,
- $r = 2$ and $w = 4$,
- $r = 1$ and $w = 4$.

In every case, one has $\dim_{\overline{\mathbb{F}}_p} J_{(\alpha,\beta)} = s = \frac{r}{(r,f_K)} = 1$ and $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_{p^4}$ (because $d = 4$), thus following (1.5) the number of irreducible representations defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}$ (having taken into account that every conjugate of $J_{(\alpha,\beta)}$ gives the same representation over $\mathbb{F}_p$).
Therefore the total number of isomorphism classes of extensions of degree p^4 having no intermediate extensions when $4 \mid f_K$ is obtained multiplying $\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}$ by the number of pairs $(\alpha, \beta) \in \mathbb{F}_{p^4}^* \times \mathbb{F}_{p^4}^*$ with $(\alpha, \beta) \notin \mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*$:

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}((p^4-1)^2-(p^2-1)^2) = \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^8-3p^4+2p^2).$$

Since $J_{(\alpha,\beta)}$ has dimension 1, the group describing the action on it is cyclic, isomorphic to the cyclic group generated by α and β in $\mathbb{F}_{p^4}^*$. It follows that the Galois group of the normal closure of each class of extensions is isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$, where C is the unique subgroup of $\mathbb{F}_{p^4}^*$ of order equal to the order of $(\alpha, \beta) \in (\mathbb{F}_{p^4}^* \times \mathbb{F}_{p^4}^*) \setminus (\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*)$.
Therefore if C is the cyclic group in $\mathbb{F}_{p^4}^*$ of fixed order c with $c \mid p^4-1$ and $c \nmid p^2-1$, then the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$ is

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}\psi(c, p^4-1)$$

where $\psi(c, p^4-1)$ is the number of elements (α, β) in $\mathbb{F}_{p^4}^* \times \mathbb{F}_{p^4}^*$ of order c. □

3.2 The total number of isomorphism classes and Galois groups when $4 \nmid f_K$

To study this case we will make extensive use of the following result.

Lemma 3.2. *Let $H_{(\alpha,\beta)}$ be the subgroup of $\mathrm{GL}(n, \mathbb{F}_{q^n})$ generated by*

$$T_\alpha = \begin{pmatrix} \alpha & & & \\ & \alpha^q & & \\ & & \ddots & \\ & & & \alpha^{q^{n-1}} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & & & \beta \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$$

with $\alpha \in \mathbb{F}_{q^n}^*$ and $\beta \in \mathbb{F}_q^*$. Then the following hold:

1. *V_β acts as power to q on T_α via conjugation, i.e. $V_\beta^{-1} T_\alpha V_\beta = T_\alpha^q$;*

2. *the subgroup of diagonal matrices is generated by T_α and V_β^n, and is cyclic isomorphic to $C := \langle \alpha, \beta \rangle \subseteq \mathbb{F}_{q^n}^*$;*

3. *$H_{(\alpha,\beta)}$ is isomorphic to a subgroup of $C \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$;*

4. *a group $\langle T_{\alpha'}, V_{\beta'} \rangle$ with $\alpha' \in \mathbb{F}_{q^n}^*$ and $\beta' \in \mathbb{F}_q^*$ is conjugate to $\langle T_\alpha, V_\beta \rangle$ if and only if $\langle \alpha', \beta' \rangle = C$ and $\beta' \equiv \beta \pmod{C^{1+q+\cdots+q^{n-1}}}$.*

Proof. (1) is an easy calculation.
(2) follows observing that since β is in $\mathbb{F}_q^*$, we have $V_\beta^n = T_\beta$.
(3) Let γ_0 be a generator of $\mathbb{F}_{q^n}^*$. We show that each group of type $\langle T_\alpha, V_\beta \rangle$ is conjugate to a subgroup of $H_0 = \langle T_{\gamma_0}, V_1 \rangle$. This group is isomorphic to $\mathbb{F}_{q^n}^* \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ via the map which sends T_{γ_0} to (γ_0, id) and V_1 to $(1, \phi_{q^{n-1}})$ (ϕ_q is the Frobenius map).
Let $\gamma \in \mathbb{F}_{q^n}^*$ be a generator of $\langle \alpha, \beta \rangle$. Let m and b be integers such that $\gamma = \gamma_0^m$ and $\beta = \gamma^b = \gamma_0^{mb}$. Since $\beta \in \mathbb{F}_q^*$, $1 + q + \cdots + q^{n-1} \mid mb$, so that we can write $\beta = \gamma_0^{j(1+q+\cdots+q^{n-1})}$. An easy calculation shows that the conjugation of $\langle T_\alpha, V_\beta \rangle =$

$\langle T_\gamma, V_\beta \rangle$ by the matrix

$$M_j = \begin{pmatrix} 1 & & & & \\ & \gamma_0^{jq} & & & \\ & & \gamma_0^{j(q+q^2)} & & \\ & & & \ddots & \\ & & & & \gamma_0^{j(q+q^2+\cdots+q^{n-1})} \end{pmatrix}$$

fixes the subgroup $\langle T_\gamma \rangle$ of the diagonal matrices and sends V_β to

$$M_j V_\beta M_j^{-1} = \begin{pmatrix} & & & & \gamma_0^{j} \\ \gamma_0^{jq} & & & & \\ & \gamma_0^{jq^2} & & & \\ & & \ddots & & \\ & & & \gamma_0^{jq^{n-1}} & \end{pmatrix} = T_{\gamma_0^j} V_1 := U_j.$$

Therefore $\langle T_\alpha, V_\beta \rangle$ is conjugate to $\langle T_\gamma, U_j \rangle \simeq \langle (\gamma_0^m, \mathrm{id}), (\gamma_0^j, \phi_{q^{n-1}}) \rangle \subseteq C \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.
(4) We first show that the conditions

$$\mathrm{o}(\langle \alpha', \beta' \rangle) = \mathrm{o}(\langle \alpha, \beta \rangle) \quad \text{and} \quad \beta' \equiv \beta \pmod{C^{1+q+\cdots+q^{n-1}}}$$

where $C = \langle \alpha, \beta \rangle$ are sufficient to guarantee that $\langle T_\alpha, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle$ are conjugate.
Since $\mathrm{o}(\langle \alpha', \beta' \rangle) = \mathrm{o}(\langle \alpha, \beta \rangle)$, $\langle T_\alpha, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle$ have the same subgroup of diagonal matrices, so that $\langle T_\alpha, V_\beta \rangle = \langle T_\gamma, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle = \langle T_\gamma, V_{\beta'} \rangle$ with $\langle \gamma \rangle = \langle \alpha, \beta \rangle = \langle \alpha', \beta' \rangle$. As seen before, $\langle T_\gamma, V_\beta \rangle$ is conjugate to $\langle T_\gamma, U_j \rangle$.
If $\beta' \equiv \beta \pmod{C^{1+q+\cdots+q^{n-1}}}$ then, with the previous notations,

$$\beta' = \gamma_0^{j(1+q+\cdots+q^{n-1})+km(1+q+\cdots+q^{n-1})} = \gamma_0^{(j+mk)(1+q+\cdots+q^{n-1})}$$

for some integer k. It follows that the conjugation by the matrix M_{j+mk} fixes $\langle T_\gamma \rangle$ and sends $V_{\beta'}$ to $T_{\gamma_0^{j+mk}} V_1 = T_{\gamma_0^{mk}} U_j \in \langle T_\gamma, U_j \rangle$; in other words $\langle T_\gamma, V_{\beta'} \rangle$ and $\langle T_\gamma, V_\beta \rangle$ are conjugate to the same subgroup of H_0, therefore they are conjugate to each other.
Finally we show that the previous conditions are necessary. Suppose that $\langle T_\alpha, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle$ are conjugate. Having both index n, the subgroups of their diagonal matrices have the same order; it follows that they are equal since they are isomorphic to the same subgroup of $\mathbb{F}_{q^n}^*$ by means of the same isomorphism. It remains to prove

that $\beta' \equiv \beta \pmod{C^{1+q+\cdots+q^{n-1}}}$, where $C = \langle \alpha, \beta \rangle = \langle \alpha', \beta' \rangle$. From what we have said above, $\langle T_\alpha, V_\beta \rangle \simeq \langle (\gamma_0^j, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle \simeq \langle (\gamma_0^{j'}, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle$. If $\langle T_\alpha, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle$ are conjugate, then

$$\langle (\gamma_0^j, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle \simeq \langle (\gamma_0^{j'}, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle,$$

in particular there exists an isomorphism

$$\psi \colon \langle (\gamma_0^j, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle \longrightarrow \langle (\gamma_0^{j'}, \phi_{q^{n-1}}), (\gamma_0^m, \mathrm{id}) \rangle$$

which fixes the elements of $\mathbb{F}_q^*$ since they correspond to matrices belonging to the center of $\mathrm{GL}(n, \mathbb{F}_{q^n})$. Moreover, we can suppose that $\psi(\langle (\gamma_0^m, \mathrm{id}) \rangle) = \langle (\gamma_0^m, \mathrm{id}) \rangle$ because there always exists a conjugation from $\langle T_\alpha, V_\beta \rangle$ to $\langle T_{\alpha'}, V_{\beta'} \rangle$ which sends diagonal matrices to diagonal matrices. This is true because the subgroup of the diagonal matrices of $\langle T_\alpha, V_\beta \rangle$ is a cyclic, maximal, of index n subgroup and there are two possibilities: there is only one subgroup in $\langle T_\alpha, V_\beta \rangle$ with these properties or, for every pairs of subgroups with these properties, there exists a conjugation from $\langle T_\alpha, V_\beta \rangle$ to itself which sends one of the two subgroups to the other.
It follows that there exists $k \in \mathbb{Z}$ such that

$$\psi((\gamma_0^j, \phi_{q^{n-1}})) = (\gamma_0^{mk}, \mathrm{id})(\gamma_0^{j'}, \phi_{q^{n-1}}).$$

Thus

$$\psi((\gamma_0^j, \phi_{q^{n-1}})^n) = ((\gamma_0^{mk}, \mathrm{id})(\gamma_0^{j'}, \phi_{q^{n-1}}))^n = (\beta' \gamma_0^{mk(1+\cdots+q^{n-1})}, \mathrm{id}).$$

But $(\gamma_0^j, \phi_{q^{n-1}})^n = (\beta, \mathrm{id}) \in \mathbb{F}_q^*$ and as such it is fixed, therefore

$$\beta = \beta' \gamma_0^{mk(1+\cdots+q^{n-1})}$$

or, equivalently,

$$\beta \equiv \beta' \pmod{C^{1+\cdots+q^{n-1}}}.$$

□

We now return to the discussion on the extensions of degree p^4 in the case $4 \nmid f_K$. We must distinguish two subcases: $2 \mid f_K$ and $2 \nmid f_K$.

$4 \nmid f_K$ and $2 \mid f_K$.
For $c \mid p^4-1$ and $c \nmid p^2-1$, we define the following function

$$\lambda(c,p) = \begin{cases} 1/3 & \text{if } p \equiv 1 \pmod 2 \text{ and } 0 < v_2(c) < v_2(p^4-1) \\ 1 & \text{otherwise} \end{cases}.$$

Theorem 3.3. *Let K be a p-adic field, f_K be its inertial degree over $\mathbb{Q}_p$ and $n_K = [K:\mathbb{Q}_p]$; suppose that $4 \nmid f_K$ and $2 \mid f_K$. Then there are*

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^8-3p^4+2p^2)$$

isomorphism classes of extensions of degree p^4 of K having no intermediate fields. Moreover, the Galois group of the normal closure of such an extension of K is either of type $\mathbb{F}_{p^4}^+ \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^4}^*$ not contained in $\mathbb{F}_{p^2}^*$ (with the natural action on $\mathbb{F}_{p^4}^+$), or of type $(\mathbb{F}_p)^4 \rtimes \mathcal{H}$, where $\mathcal{H} \subseteq \mathrm{GL}(4,\mathbb{F}_p)$ is isomorphic to a non-abelian subgroup of $\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})$ such that the intersection with $\mathbb{F}_{p^4}^*$ is not contained in $\mathbb{F}_{p^2}^*$.
In particular,

- *for every integer c dividing p^4-1 but not p^2-1, if C is the cyclic subgroup of $\mathbb{F}_{p^4}^*$ of order c, then there are*

  $$n(c) = \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}\psi(c,p^2-1)$$

  isomorphism classes of p^4-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$;

- *for every non-abelian subgroup $\mathcal{H} \subseteq \mathrm{GL}(4,\mathbb{F}_p)$ isomorphic to a subgroup Z of $\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})$ such that $C = Z \cap \mathbb{F}_{p^4}^* \not\subseteq \mathbb{F}_{p^2}^*$, if C has order c then there are*

  $$n(\mathcal{H}) = \begin{cases} \frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}\lambda(c,p)\psi(c,p^2-1) & \text{if } C \to Z \text{ splits} \\ \frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}(1-\lambda(c,p))\psi(c,p^2-1) & \text{if } C \to Z \text{ does not split} \end{cases}$$

  isomorphism classes of p^4-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $(\mathbb{F}_p)^4 \rtimes \mathcal{H}$.

Proof. By equation (3.1) since $2 \parallel f_K$, we can have

- $r = 4$ and $w = 1, 2 \Longrightarrow s = 2$, $d = 2$
- $r = 2$ and $w = 4 \Longrightarrow s = 1$, $d = 4$
- $r = 1$ and $w = 4 \Longrightarrow s = 1$, $d = 4$

With the same arguments as above, one finds that the total number of isomorphism classes of extensions of degree p^4 having no intermediate extensions when $4 \nmid f_K$ and $2 \mid f_K$ is

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}(p^4-p^2)(p^2-1) + \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^2-1)(p^4-p^2) = \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^8-3p^4+2p^2).$$

Observe that the coefficient $1/4$ has different meaning in the two addends: in the first addend is due to the fact that each $J_{(\alpha,\beta)}$ has two conjugates but it can be obtained starting from the two different pairs (α, β) and $(\alpha^{p^2}, \beta^{p^2})$, in the second one each $J_{(\alpha,\beta)}$ is obtained only by a unique pair but it has four conjugates over $\mathbb{F}_p$. As usual when $s = 1$, it is easy to find the Galois group of the normal closure of the corresponding class of extensions. In fact if $r = 1$ or $r = 2$, the group acting on the representation is cyclic of order equal to the order of (α, β) in $\mathbb{F}_{p^2}^* \times (\mathbb{F}_{p^4}^* \setminus \mathbb{F}_{p^2}^*)$. Therefore, as before, if C is the cyclic group of order c in $\mathbb{F}_{p^4}^*$ with $c \mid p^4 - 1$ and $c \nmid p^2 - 1$, then the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes C$ is

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}\psi(c, p^2-1)$$

where $\psi(c, p^2-1)$ is the number of elements (α, β) in $(\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^4}^*) \setminus (\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*)$ of order c.

Assume now $r = 4$, then we must have $w = 1$ or $w = 2$, that is $\alpha \in \mathbb{F}_{p^4}^* \setminus \mathbb{F}_{p^2}^*$ and $\beta \in \mathbb{F}_{p^2}^*$. In these cases we have $s = \dim_{\overline{\mathbb{F}}_p} J_{(\alpha,\beta)} = 2$ and the group acting on the representation is not abelian. It turns out that $d = \operatorname{lcm}(w, (r, f_K)) = 2$, so $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_{p^2}$ and for every pairs (α, β) there are $\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}$ irreducible representations over $\mathbb{F}_p$ containing a representation isomorphic to $J_{(\alpha,\beta)}$. Since we are assuming that $4 \nmid f_K$ but $2 \mid f_K$, the action on $J_{(\alpha,\beta)}$ is described by the matrices

$$T_\alpha = \begin{pmatrix} \alpha & \\ & \alpha^{p^2} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & \beta \\ 1 & \end{pmatrix},$$

with $\alpha \in \mathbb{F}_{p^4}^* \setminus \mathbb{F}_{p^2}^*$ and $\beta \in \mathbb{F}_{p^2}^*$.
We want to count the number of pairs (α', β') which lead to a Galois group isomorphic to that induced by $\langle T_\alpha, V_\beta \rangle$, i.e. such that

$$(\mathbb{F}_{p^2})^2 \rtimes \langle T_{\alpha'}, V_{\beta'} \rangle \simeq (\mathbb{F}_{p^2})^2 \rtimes \langle T_\alpha, V_\beta \rangle.$$

Observe that our group satisfies the hypothesis of Lemma 3.2 with $q = p^2$ and $n = 2$, thus $\langle T_\alpha, V_\beta \rangle$ is isomorphic to a subgroup of $C \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})$ with $C = \langle \alpha, \beta \rangle \subseteq \mathbb{F}_{p^4}^*$; moreover $\langle T_\alpha, V_\beta \rangle$ and $\langle T_{\alpha'}, V_{\beta'} \rangle$ are conjugate if and only if $\langle \alpha', \beta' \rangle = \langle \alpha, \beta \rangle = C$ and $\beta' \equiv \beta \pmod{C^{p^2+1}}$.
It follows that the Galois group is identified by the order of C and the class of β in $(C \cap \mathbb{F}_{p^2}^*)/C^{p^2+1}$. Note that $\beta \in C^{p^2+1}$ if and only if the map $C \hookrightarrow \langle T_\alpha, V_\beta \rangle$ splits. Indeed this map splits if and only if β has a square root in C which is equivalent to say that β has a (p^2+1)-root in C.
Let c be the order of C; clearly $c \mid p^4 - 1$ but $c \nmid p^2 - 1$. Since $(p^2+1, p^2-1) = 2$ (or 1 if $p = 2$), one has

$$\left| \frac{C \cap \mathbb{F}_{p^2}^*}{C^{p^2+1}} \right| = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 2 \text{ and } 0 < v_2(c) < v_2(p^4 - 1) \\ 1 & \text{otherwise.} \end{cases}$$

If $(C \cap \mathbb{F}_{p^2}^*)/C^{p^2+1}$ is trivial, then all the possible β's are equivalent mod C^{p^2+1}, therefore there are $\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}\psi(c, p^2-1)$ classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes \langle T_\alpha, V_\beta \rangle$.
Suppose now that $(C \cap \mathbb{F}_{p^2}^*)/C^{p^2+1}$ has order 2 and let 2^k be the largest power of 2 dividing c. Then $\beta \in C^{p^2+1}$ if and only if $\mathrm{o}(\beta)$ is not divisible by a power of 2 greater than $\frac{2^k}{(2^k, p^2+1)} = 2^{k-1}$ (note that $2 \| p^2+1$). It follows that to count the number of pairs (α, β) with $\beta \in C^{p^2+1}$, it suffices to look at the 2-part of $\mathbb{F}_{p^4}^* \times \mathbb{F}_{p^2}^*$. If C_n denotes the cyclic group of order n, the 2-part of $\mathbb{F}_{p^4} \times \mathbb{F}_{p^2}$ is exactly $C_{2^{z+1}} \times C_{2^z}$ where $2^z \| p^2 - 1$. Therefore we have $k \leq z$, and $\beta \in C^{p^2+1}$ if and only if the 2-component of (α, β) is of type (x, y) with $\mathrm{o}(x) = 2^k > \mathrm{o}(y)$; this happens in 1/3 of the pairs of correct order.
Thus $\lambda(c,p)\psi(c, p^2-1)$ is the number of pairs (α, β) in $\mathbb{F}_{p^4}^* \times \mathbb{F}_{p^2}^*$ such that α and β generate a cyclic group of order c and $\beta \in C^{p^2+1}$, while $(1 - \lambda(c,p))\psi(c, p-1)$ is the number of the pairs in the same group which generate the same cyclic C but with $\beta \notin C^{p^2+1}$. Multiplying these values by $\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}$, we obtain the number of

isomorphism classes of extensions whose normal closure has a fixed Galois group. From the above it is clear that the possible groups of matrices which can appear in the representations are the non-abelian subgroups of $\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})$ such that the intersection with $\mathbb{F}_{p^4}^*$ is not contained in $\mathbb{F}_{p^2}^*$. If Z is such a subgroup, $C = Z \cap \mathbb{F}_{p^4}^*$ and $c = \mathrm{o}(C)$ (so $c \nmid p^2 - 1$), then there are

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}\lambda(c,p)\psi(c,p^2-1)$$

classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes Z$ if $C \hookrightarrow Z$ splits, and

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}(1-\lambda(c,p))\psi(c,p^2-1)$$

if $C \hookrightarrow Z$ does not split. □

$4 \nmid f_K$ and $2 \nmid f_K$.

Again we will use the function ψ introduced above which maps each pair of natural numbers (a,b) to the number of elements of order a in $C_a \times C_b$. Moreover we define two functions that will appear in what follows.

For $c \mid p^4 - 1$ and $c \nmid p^2 - 1$, set

$$\lambda(c,p) = \begin{cases} 1/6 & \text{if } p \equiv 1 \pmod 4 \text{ and } 1 < v_2(c) < v_2(p^4-1) - 1 \\ 1/3 & \text{if } v_2(c) = 1 \\ 1/2 & \text{if } p \equiv 3 \pmod 4 \text{ and } 1 < v_2(c) < v_2(p^4-1) \\ & \text{or, } p \equiv 1 \pmod 4 \text{ and } v_2(c) = v_2(p^4-1) - 1 \\ 1 & \text{otherwise} \end{cases}$$

and, for $c_1 \mid p^2 - 1$ and $c_2 \mid (p+1, c_1)$, if $c_1 = 2^{t_0}\prod_{i=1}^r p_i^{t_i}$, $c_2 = 2^{w_0}\prod_{i=1}^r p_i^{w_i}$ and

$p-1 = 2^{k_0}\prod_{i=1}^{r} p_i^{k_i}\prod q_j^{h_j}$, set

$$\nu(c_1,c_2,p-1) = \frac{1}{2^{t_0+1}-1}\begin{cases} 2^{t_0}-1 & \text{if } k_0=1,\ w_0=t_0 \\ 2^{w_0-1} & \text{if } k_0=1,\ w_0<t_0 \\ 2^{t_0-1} & \text{if } k_0>1,\ t_0<k_0+1,\ w_0=0 \\ 2^{t_0-w_0} & \text{if } k_0>1,\ t_0<k_0+1,\ w_0>0 \\ 2^{k_0-1} & \text{if } k_0>1,\ t_0=k_0+1,\ 0\le w_0\le 1 \\ 3\cdot 2^{k_0-1} & \text{if } k_0>1,\ t_0=k_0+1,\ w_0=2 \\ 2^{k_0-w_0-1} & \text{if } k_0>1,\ t_0=k_0+1,\ w_0>2 \\ 1 & \text{otherwise} \end{cases}.$$

Theorem 3.4. *Let K be a p-adic field, f_K be its inertial degree over $\mathbb{Q}_p$ and $n_K = [K:\mathbb{Q}_p]$; suppose $2 \nmid f_K$. Then there are*

$$\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^8-p^5-3p^3+3p^2)$$

isomorphism classes of extensions of degree p^4 of K having no intermediate fields. The Galois group of the normal closure of these extensions is $(\mathbb{F}_p^+)^4 \rtimes \mathcal{H}$ where $\mathcal{H} \subseteq \mathrm{GL}(4,\mathbb{F}_p)$ satisfies one of the following:

1. *$\mathcal{H} \simeq C$ with $C < \mathbb{F}_{p^4}^*$ and $C \not< \mathbb{F}_{p^2}^*$;*

2. *$\mathcal{H} \simeq Z$ with Z non-abelian subgroup of $\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)$ such that $C = Z \cap \mathbb{F}_{p^4}^*$ is not contained in $\mathbb{F}_{p^2}^*$;*

3. *$\mathcal{H} \simeq B$ with B non-abelian subgroup of $(\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*/\mathbb{F}_p^*) \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ (where $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acts non-trivially only on the first factor) such that $B \cap (\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*/\mathbb{F}_p^*) = C_1 \times C_2$ is not cyclic and $C_2 < C_1$.*

Let $n(\mathcal{H})$ be the number of isomorphism classes of extensions whose Galois group of the normal closure is $(\mathbb{F}_p^+)^4 \rtimes \mathcal{H}$, then

(a) for all $\mathcal{H}$ as in 1, if $\mathrm{o}(C) = c$,

$$n(\mathcal{H}) = \frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}\psi(c, p-1);$$

(b) for all $\mathcal{H}$ as in 2, if $\mathrm{o}(C) = c$ and

- *$p \not\equiv 1 \pmod 4$ or $p \equiv 1 \pmod 4$ and, either $v_2(c) = 1$ or $v_2(c) = v_2(p^4-1)-1$, then*

$$n(\mathcal{H}) = \begin{cases} \frac{1}{4}\frac{p^{4n_K}-1}{p-1}\lambda(c,p)\psi(c,p-1) & \text{if } C \hookrightarrow Z \text{ splits} \\ \frac{1}{4}\frac{p^{4n_K}-1}{p-1}(1-\lambda(c,p))\psi(c,p-1) & \text{if } C \hookrightarrow Z \text{ does not split} \end{cases}$$

- *$p \equiv 1 \pmod 4$ and $1 < v_2(c) < v_2(p^4-1)-1$, then*

$$n(\mathcal{H}) = \begin{cases} \frac{1}{4}\frac{p^{4n_K}-1}{p-1}\frac{1}{6}\psi(c,p-1) & \text{if } C \hookrightarrow Z \cap (\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})) \\ & \text{splits} \\ \frac{1}{4}\frac{p^{4n_K}-1}{p-1}\frac{1}{3}\psi(c,p-1) & \text{if } C \hookrightarrow Z \cap (\mathbb{F}_{p^4}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})) \\ & \text{does not split} \end{cases}$$

(c) for all $\mathcal{H}$ as in 3, if $\mathrm{o}(C_1) = c_1 = 2^{t_0}\prod_{i=1}^r p_i^{t_i}$, $\mathrm{o}(C_2) = c_2 = 2^{w_0}\prod_{i=1}^r p_i^{w_i}$ and $p-1 = 2^{k_0}\prod_{i=1}^r p_i^{k_i}\prod q_j^{h_j}$, then

$$n(\mathcal{H}) = \prod_{\substack{1\le i\le r \\ k_i>0 \wedge w_i=0 \\ k_i=0 \wedge w_i=t_i}} \frac{p_i^{t_i}}{2p_i^{t_i}-1} \cdot \prod_{\substack{1\le i\le r \\ k_i>0 \\ w_i>0}} \frac{p_i^{t_i-w_i-1}(p_i-1)}{2p_i^{t_i}-1} \cdot \prod_{\substack{1\le i\le r \\ k_i=0 \\ w_i<t_i}} \frac{p_i^{w_i-1}(p_i-1)}{2p_i^{t_i}-1}$$
$$\cdot \psi(c_1, p^2-1) \cdot \nu(c_1, c_2, p-1).$$

Proof. In this case, we can have

- $r = 4$ and $w = 1 \Longrightarrow s = 4$, $d = 1$
- $r = 2$ and $w = 2 \Longrightarrow s = 2$, $d = 2$
- $r = 1$ and $w = 4 \Longrightarrow s = 1$, $d = 4$

It follows that the total number of isomorphism classes of extensions of degree p^4

having no intermediate extensions when $4 \nmid f_K$ and $2 \nmid f_K$ is

$$\frac{1}{4}\frac{p^{4n_K}-1}{p-1}(p^4-p^2)(p-1)+\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}(p^2-p)(p^2-p)+\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p-1)(p^4-p^2)$$
$$=\frac{1}{4}\frac{p^{4n_K}-1}{p^4-1}(p^8-p^5-3p^3+3p^2).$$

Observe that as above the coefficient $1/4$ has different meaning in each addend. In particular, in the first addend the representation $J_{(\alpha,\beta)}$ has dimension 4 and is already defined over $\mathbb{F}_p$, so the factor $1/4$ is due to the fact that the pairs (α^{p^i},β), $i=1,\dots,4$, give the same representation; in the second addend $J_{(\alpha,\beta)}$ has 2 conjugates over $\mathbb{F}_p$, each of which can be defined starting from two different pairs; finally, in the third addend $J_{(\alpha,\beta)}$ has 4 conjugates and this explains the presence of the factor $1/4$.

The case $r=1$ and $w=4$ is the same as when $4 \nmid f_K$ and $2 \mid f_K$, so claim (a) is done.

Assume now $r=4$ and $w=1$. Then $s=\dim_{\overline{\mathbb{F}}_p} J_{(\alpha,\beta)}=4$ and the group acting on the representation is non-abelian. Since $d=1$, $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_p$, therefore following (1.5) for every pairs (α,β) there are $\frac{1}{4}\frac{p^{4n_K}-1}{p-1}$ irreducible representations over $\mathbb{F}_p$ isomorphic to $J_{(\alpha,\beta)}$. The action on $J_{(\alpha,\beta)}$ is described by the matrices

$$T_\alpha=\begin{pmatrix}\alpha & & & \\ & \alpha^p & & \\ & & \alpha^{p^2} & \\ & & & \alpha^{p^3}\end{pmatrix},\quad V_\beta=\begin{pmatrix} & & & \beta \\ 1 & & & \\ & 1 & & \\ & & 1 & \end{pmatrix},$$

with $\alpha\in\mathbb{F}_{p^4}^*\setminus\mathbb{F}_{p^2}^*$ and $\beta\in\mathbb{F}_p^*$.
We want to count the number of pairs (α',β') such that the representations isomorphic to $J_{(\alpha',\beta')}$ correspond to extensions with Galois group isomorphic to that given by $J_{(\alpha,\beta)}$.
Applying Lemma 3.2 with $q=p$ and $n=4$, we have that $\langle T_\alpha,V_\beta\rangle$ is isomorphic to a subgroup of $C\rtimes\mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)$ with $C=\langle\alpha,\beta\rangle\subseteq\mathbb{F}_{p^4}^*$, and $\langle T_\alpha,V_\beta\rangle$ is conjugate to $\langle T_{\alpha'},V_{\beta'}\rangle$ if and only if $\langle\alpha',\beta'\rangle=\langle\alpha,\beta\rangle$ and $\beta'\equiv\beta(\mathrm{mod}\ C^{p^3+p^2+p+1})$. This means that the Galois group is identified by the order c of C and by the class of β in $(C\cap\mathbb{F}_p^*)/C^{p^3+p^2+p+1}$.

As usual $\beta \in C^{p^3+p^2+p+1}$ if and only if the map $C \hookrightarrow \langle T_\alpha, V_\beta \rangle$ splits.
Since

$$(p-1, p^3+p^2+p+1) = \begin{cases} 1 & \text{if } p = 2 \\ 2 & \text{if } p \equiv 3 \pmod 4 \\ 4 & \text{if } p \equiv 1 \pmod 4 \end{cases},$$

we have

$$\left| \frac{C \cap \mathbb{F}_p^*}{C^{p^3+p^2+p+1}} \right| = \begin{cases} 4 & \text{if } p \equiv 1 \pmod 4 \text{ and } 1 < v_2(c) < v_2(p^4-1) - 1 \\ 2 & \text{if } p \equiv 3 \pmod 4 \text{ and } 0 < v_2(c) < v_2(p^4-1), \\ & \text{or } p \equiv 1 \pmod 4 \text{ and, either } v_2(c) = 1 \text{ or} \\ & v_2(c) = v_2(p^4-1) - 1 \\ 1 & \text{otherwise} \end{cases}$$

If $|\frac{C \cap \mathbb{F}_p^*}{C^{p^3+p^2+p+1}}| = 1$, i.e. there is only one class mod $C^{p^3+p^2+p+1}$, then all the pairs (α', β') such that $\langle \alpha', \beta' \rangle = C$ give isomorphic Galois groups, thus in this case there are $\frac{1}{4}\frac{p^{4n_K}-1}{p-1}\psi(c, p-1)$ isomorphism classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^4}^+ \rtimes \langle T_\alpha, V_\beta \rangle$.
Suppose that $|\frac{C \cap \mathbb{F}_p^*}{C^{p^3+p^2+p+1}}| = 4$. Then, in order to classify the pairs $(\alpha, \beta) \in \mathbb{F}_{p^4}^* \times \mathbb{F}_p^*$ which give different Galois groups, it suffices to look at the 2-part of $\mathbb{F}_{p^4}^* \times \mathbb{F}_p^*$. It is $C_{2^{m_1+m_2+z}} \times C_{2^z}$ where $2^z \| p-1$, $2^{m_1} \| p+1$ and $2^{m_2} \| p^2+1$.
Since $p \equiv 1 \pmod 4$ we have $m_1 = m_2 = 1$, therefore the 2-part of $\mathbb{F}_{p^4}^* \times \mathbb{F}_p^*$ is $C_{2^{z+2}} \times C_{2^z}$ with $z \geq 2$.
Thus if $2^k \| c$ one has $2 \leq k \leq z$, and $\beta \in C^{p^3+p^2+p+1}$ if and only if its order is not divisible by a power of 2 greater than $\frac{2^k}{(2^k, p^3+p^2+p+1)} = 2^{k-2}$; moreover $\beta (\bmod C^{p^3+p^2+p+1})$ has order 2 if $2^{k-1} \| \mathrm{o}(\beta)$ and $\beta (\bmod C^{p^3+p^2+p+1})$ has order 4 if $2^k \| \mathrm{o}(\beta)$.
It follows that $\beta \in C^{p^3+p^2+p+1}$ if and only if the 2-component of (α, β) is of type (x, y) with $\mathrm{o}(x) = 2^k$ and $\mathrm{o}(y) \leq 2^{k-2}$. This happens in $1/6 = \lambda(c, p)$ of the elements of correct order. For the same number of pairs, $\beta (\bmod C^{p^3+p^2+p+1})$ has order 2, and clearly for 2/3 of the pairs of correct order $\beta (\bmod C^{p^3+p^2+p+1})$ has order 4.
Thus, when $p \equiv 1 \pmod 4$ and $1 < v_2(c) < v_2(p^4-1) - 1$, the pairs (α, β) such that $\beta \notin C^{p^3+p^2+p+1}$ must be divided in two classes according to the order of $\beta (\bmod C^{p^3+p^2+p+1})$. Indeed, $1 - \lambda(c, p) = \frac{5}{6}$ and we have $\frac{1}{6}\psi(c, p-1)$ pairs (α, β)

such that the group C generated by α and β has order c and $\beta (\mathrm{mod}\ C^{p^3+p^2+p+1})$ has order 2, and $\frac{2}{3}\psi(c, p-1)$ pairs with $\beta (\mathrm{mod}\ C^{p^3+p^2+p+1})$ of order 4. Since there are two classes of this order, we must divide by 2 getting $\frac{1}{3}\psi(c, p-1)$.
Suppose now $|\frac{C \cap \mathbb{F}_p^*}{C^{p^3+p^2+p+1}}| = 2$, thus the pairs (α, β) such that $\langle \alpha, \beta \rangle = C$ can be divided in only two classes depending on $\beta \in C^{p^3+p^2+p+1}$ or $\beta \notin C^{p^3+p^2+p+1}$.
If $p \equiv 3 \pmod 4$ and $2^k \| c$, then $k \geq 1$ and, when we write the 2-part of $\mathbb{F}_{p^4}^* \times \mathbb{F}_p^*$ as $C_{2^{m_1+m_2+z}} \times C_{2^z}$ (as in the previous case), we have necessarily $z = 1$, $m_2 = 1$ and $m_1 \geq 2$, while k is such that $1 \leq k \leq m_1 + 1$. It follows that $\beta \in C^{p^3+p^2+p+1}$ if and only if its order is not divisible by a power of 2 greater than $\frac{2^k}{(2^k, p^3+p^2+p+1)} = 1$, i.e. if and only if the 2-component of (α, β) is of type $(x, 1)$ with $\mathrm{o}(x) = 2^k$. This happens for $1/2$ of the pairs of correct order if $k > 1$ and for $1/3$ of them if $k = 1$.
If $p \equiv 1 \pmod 4$ and $v_2(c) = 1$, then, with the previous notations, we have $m_1 = m_2 = k = 1$ and $z \geq 2$; therefore $\beta \in C^{p^3+p^2+p+1}$ if and only if the 2-component of (α, β) is of type $(x, 1)$ with $\mathrm{o}(x) = 2$ and this happens for $1/3$ of the elements of correct order.
Finally, if $p \equiv 1 \pmod 4$ and $v_2(c) = v_2(p^4 - 1) - 1$, i.e. $k = z + 2 - 1 = z + 1$ in the previous notations, then in order that β is in $C^{p^3+p^2+p+1}$, the 2-component of (α, β) must be of type (x, y) with $\mathrm{o}(x) = 2^{z+1}$ and $\mathrm{o}(y) \leq 2^{z-1}$. This happens for $1/2$ of the pairs (x, y) of correct order.
Then $\lambda(c, p)\psi(c, p-1)$ is the number of pairs (α, β) such that the group C generated by α and β has order c and $\beta \in C^{p^3+p^2+p+1}$, while $(1 - \lambda(c, p))\psi(c, p-1)$ counts the same pairs but with $\beta \notin C^{p^3+p^2+p+1}$.
Note that, while $\beta \in C^{p^3+p^2+p+1}$ (i.e. $\beta (\mathrm{mod}\ C^{p^3+p^2+p+1})$ of order 1) is equivalent to the condition that $C \hookrightarrow \langle T_\alpha, V_\beta \rangle$ splits, $\beta (\mathrm{mod}\ C^{p^3+p^2+p+1})$ of order 2 is equivalent to $C \hookrightarrow \langle T_\alpha, V_\beta^2 \rangle$ splitting.
Multiplying by $\frac{1}{4}(p^{4n_K} - 1)/(p-1)$, we obtain the number of isomorphism classes of extensions whose normal closure has a fixed Galois group.
From above, it is clear that every group $\langle T_\alpha, V_\beta \rangle$ with $\alpha \in \mathbb{F}_{p^4}^* \setminus \mathbb{F}_{p^2}^*$ and $\beta \in \mathbb{F}_p^*$ is isomorphic to a subgroup of $C \rtimes \mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)$ for some $C < \mathbb{F}_{p^4}^*$ not contained in $\mathbb{F}_{p^2}^*$. Summarizing all the informations we obtain the claim (b).

Finally, it remains to consider the case $r = 2$; this implies $w = 2$, i.e. $\alpha, \beta \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$. It follows that $s = \dim_{\overline{\mathbb{F}}_p} J_{(\alpha,\beta)} = 2$ and, since $d = 2$, for all possible pairs (α, β)

there are $\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}$ representations over $\mathbb{F}_p$ containing a representation isomorphic to $J_{(\alpha,\beta)}$.

The action on $J_{(\alpha,\beta)}$ is given by the matrices

$$T_\alpha = \begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & \beta \\ 1 & \end{pmatrix},$$

with $\alpha, \beta \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$.

The representations isomorphic to $J_{(\alpha,\beta)}$ give rise to $\frac{1}{4}\frac{p^{4n_K}-1}{p^2-1}$ isomorphism classes of extensions of degree p^4 having no intermediate extensions whose normal closure has the Galois group isomorphic to $(\mathbb{F}_{p^2}^+)^2 \rtimes \langle T_\alpha, V_\beta \rangle$. We have to count the number of pairs (α', β'), with $\alpha', \beta' \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$, such that the representations isomorphic to $J_{(\alpha',\beta')}$ yield extensions whose normal closure has Galois group isomorphic to $(\mathbb{F}_{p^2}^+)^2 \rtimes \langle T_\alpha, V_\beta \rangle$, i.e. such that $\langle T_{\alpha'}, V_{\beta'} \rangle$ is conjugate to $\langle T_\alpha, V_\beta \rangle$.

Note that in this case we cannot use Lemma 3.2 because $q = p$ and $\beta \notin \mathbb{F}_p^*$.

It is easy to see that, if $a = \mathrm{o}(\alpha)$ and $b = \mathrm{o}(\beta)$ then the group $\langle T_\alpha, V_\beta^2 \rangle$ of the diagonal matrices of $\langle T_\alpha, V_\beta \rangle$ is an abelian not cyclic subgroup of index 2 isomorphic to

$$\frac{\mathbb{Z}}{[a,b]\mathbb{Z}} \times \frac{\mathbb{Z}}{\frac{(a,b)}{(a,b,p-1)}\mathbb{Z}},$$

where we used the standard notation $[a, b]$ to denote the least common multiple of a and b.

Observe that every conjugation of $\langle T_\alpha, V_\beta \rangle$ fixes the subgroup of the multiples of identity; this leads to the necessary condition

$$[b', (a', p-1)] = [b, (a, p-1)]. \tag{3.2}$$

Moreover the subgroup of the squares

$$S = \langle \begin{pmatrix} \alpha^2 & \\ & \alpha^{2p} \end{pmatrix}, \begin{pmatrix} \beta & \\ & \beta \end{pmatrix} \rangle$$

is isomorphic to $\frac{\mathbb{Z}}{[\frac{a}{2},b]\mathbb{Z}} \times \frac{\mathbb{Z}}{\frac{(a,b)}{(a,b,p-1)}\mathbb{Z}}$ if $2 \mid a$ and it is equal to the subgroup of the diagonal matrices if $2 \nmid a$. Clearly S is sent into the subgroup S' of the squares of $\langle T_{\alpha'}, V_{\beta'} \rangle$, in particular $V_{\beta'}^2$ is the image of $V_\beta^{2k} T_\alpha^{2h}$ for some integers h, k. This implies that

$$\frac{\langle \beta, \alpha^2 \rangle}{\langle \alpha^2 \rangle} = \frac{\langle \beta', \alpha'^2 \rangle}{\langle \alpha'^2 \rangle}. \tag{3.3}$$

But (3.2) implies that the order of β can be changed only up to divisors of $(a, p-1)$, i.e. the elements of $\langle\alpha\rangle$ that can appear as factors of β' are those of $\langle\alpha^{\frac{a}{(a,p-1)}}\rangle$. It follows that the condition which has to be satisfied is

$$\frac{\langle\beta, \alpha^{\frac{a}{(a,p-1)}}{}^2\rangle}{\langle\alpha^{\frac{a}{(a,p-1)}}{}^2\rangle} = \frac{\langle\beta', \alpha'^{\frac{a}{(a,p-1)}}{}^2\rangle}{\langle\alpha'^{\frac{a'}{(a',p-1)}}{}^2\rangle}. \tag{3.4}$$

On the other hand, equating the orders of the subgroups of the squares one gets

$$[a, b] = [a', b'] \quad \text{and} \quad \frac{(a, b)}{(a, b, p-1)} = \frac{(a', b')}{(a', b', p-1)}. \tag{3.5}$$

Conditions (3.4) and (3.5) imply that if $\langle T_\alpha, V_\beta\rangle$ and $\langle T_{\alpha'}, V_{\beta'}\rangle$ are conjugate then it must be true that

$$\langle\alpha, \beta\rangle = \langle\alpha', \beta'\rangle \quad \text{and} \quad \frac{\langle\beta, \alpha^{\frac{a}{(a,p-1)}}{}^2\rangle}{\langle\alpha^{\frac{a}{(a,p-1)}}{}^2\rangle} = \frac{\langle\beta', \alpha'^{\frac{a}{(a,p-1)}}{}^2\rangle}{\langle\alpha'^{\frac{a'}{(a',p-1)}}{}^2\rangle}. \tag{3.6}$$

Observe that $\langle\alpha^{\frac{a}{(a,p-1)}}\rangle^2$ has order $(a, p-1)$ if $2 \nmid (a, p-1)$ and $(a, p-1)/2$ if $2 \mid (a, p-1)$.

Now we show the converse, i.e. if conditions (3.6) hold then $\langle T_\alpha, V_\beta\rangle$ and $\langle T_{\alpha'}, V_{\beta'}\rangle$ are conjugate. Let γ_0 be a generator of $\mathbb{F}^*_{p^2}$. We construct a conjugation which embeds $\langle T_\alpha, V_\beta\rangle$ in

$$H_0 = \langle \begin{pmatrix} \gamma_0 & \\ & \gamma_0^p \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} & \gamma_0 \\ 1 & \end{pmatrix} \rangle$$

Denote by $\mathcal{D}$ the subgroup of the diagonal matrices of $\langle T_\alpha, V_\beta\rangle$. Let $\gamma = \gamma_0^m$ be a generator of $\langle\alpha, \beta\rangle \subseteq \mathbb{F}^*_{p^2}$. Suppose that $\alpha = \gamma^i$ and $\beta = \gamma^j$. We distinguish two cases: $2 \mid j$ and $2 \nmid j$. If $2 \mid j$ then the conjugation by the matrix

$$M_j = \begin{pmatrix} 1 & \\ & \gamma^{j/2} \end{pmatrix}$$

sends $\langle T_\alpha, V_\beta\rangle$ into the subgroup

$$\langle \mathcal{D}, \begin{pmatrix} & \gamma^{j/2} \\ \gamma^{j/2} & \end{pmatrix} \rangle$$

of H_0.

Consider now $\alpha', \beta' \in \mathbb{F}^*_{p^2}$ which satisfy conditions (3.6). Then $\beta' = \gamma^{jk+i2\frac{a}{(a,p-1)}h}$

for some integers k, h such that

$$\left(k, \frac{b}{(b, \mathrm{o}\langle \alpha^{\frac{a}{(a,p-1)}2}\rangle)}\right) = 1.$$

Observe that k is defined mod b and that $2 \mid j$ if and only if $2 \mid jk + i2\frac{a}{(a,p-1)}h$, this is true since the second addend is always even and $2 \nmid j$ means that $v_2(b) \geq v_2(a)$ which implies, if $v_2(b) > 0$, that $2 \Big| \frac{b}{(b,\mathrm{o}\langle \alpha^{\frac{a}{(a,p-1)}}\rangle^2)}$, thus $2 \nmid jk$. On the other hand, if $v_2(b) = 0$ then every class mod b can be represented by an odd integer and thus we can suppose $2 \nmid k$.

The matrix $M_{jk+i2\frac{a}{(a,p-1)}h}$ fixes the subgroup of the diagonal matrices and sends $V_{\beta'}$ in

$$\begin{pmatrix} & \gamma^{\frac{jk+i2\frac{a}{(a,p-1)}h}{2}} \\ \gamma^{\frac{jk+i2\frac{a}{(a,p-1)}h}{2}} & \end{pmatrix},$$

therefore it sends $\langle T_{\alpha'}, V_{\beta'}\rangle$ in

$$\langle \mathcal{D}, \begin{pmatrix} & \gamma^{\frac{jk+i2\frac{a}{(a,p-1)}h}{2}} \\ \gamma^{\frac{jk+i2\frac{a}{(a,p-1)}h}{2}} & \end{pmatrix}\rangle$$

which is the same subgroup of H_0 conjugate to $\langle T_\alpha, V_\beta\rangle$. If $2 \nmid j$ then the conjugation by the matrix M_{j-1} sends $\langle T_\alpha, V_\beta\rangle$ into the subgroup generated by $\mathcal{D}$ and $\begin{pmatrix} & \gamma^{\frac{j-1}{2}+1} \\ \gamma^{\frac{j-1}{2}} & \end{pmatrix}$. Again if we change β with β' as above, we obtain the same subgroup of H_0, i.e. if conditions (3.6) hold than $\langle T_\alpha, V_\beta\rangle$ and $\langle T_{\alpha'}, V_{\beta'}\rangle$ are conjugate. It remains to count the number of pairs (α', β') satisfying conditions (3.6).

Let $c_1 = [a, b]$ and, $c_2 = \frac{b}{(b,(a,p-1)/2)}$ or $c_2 = \frac{b}{(b,(a,p-1))}$ according to the cases $2 \mid a$ and $2 \nmid a$. Conditions (3.6) can be written as

$$\mathrm{o}(\langle \alpha', \beta'\rangle) = c_1 \quad \text{and} \quad \mathrm{o}(\langle \beta', \alpha'^{\frac{a}{(a,p-1)}2}\rangle / \langle \alpha'^{\frac{a'}{(a',p-1)}2}\rangle) = c_2, \tag{3.7}$$

they are sufficient to identify the conjugation class of $\langle T_\alpha, V_\beta\rangle$.

Note that $2 \mid a$ if and only if $2 \mid a'$.

Since $c_2 \mid c_1$ we have

$$\begin{aligned} c_1 &= 2^{t_0} p_1^{t_1} \cdots p_r^{t_r} \\ c_2 &= 2^{w_0} p_1^{w_1} \cdots p_r^{w_r} \\ p - 1 &= 2^{k_0} p_1^{k_1} \cdots p_r^{k_r} q_1^{h_1} \cdots q_v^{h_v} \end{aligned}$$

where $k_0, t_i > 0$ for $1 \leq i \leq r$ and $t_0, w_i, k_j \geq 0$ for $0 \leq i \leq r$ and $1 \leq j \leq r$. Clearly $w_i \leq t_i$ for all i and $t_i \leq k_i$ for all $i \neq 0$ such that $k_i > 0$.
If α' and β' satisfy (3.7), then $a' = \mathrm{o}(\alpha')$ and $b' = \mathrm{o}(\beta')$ are divisors of c_1, thus we can write them as

$$a' = 2^{\gamma_0} p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$
$$b' = 2^{\delta_0} p_1^{\delta_1} \cdots p_r^{\delta_r}$$

with $0 \leq \gamma_i, \delta_i \leq t_i$ for all i. Conditions (3.7) means that we must have

$$\begin{cases} \max\{\gamma_i, \delta_i\} = t_i & \text{for all } i \\ \delta_i - \min\{\delta_i, \min\{\gamma_i, k_i\}\} = w_i & \text{for all } i \neq 0 \\ \delta_0 - \min\{\delta_0, \min\{\gamma_0, k_0\} - 1\} = w_0 & \text{if } 2 \mid a \\ \delta_0 - \min\{\delta_0, \min\{\gamma_0, k_0\} = w_0 & \text{if } 2 \nmid a \end{cases} \tag{3.8}$$

We now analyze what these imply on the p_i-part of (α', β').
For $i = 1 \ldots r$, if $k_i > 0$ then $\min\{\gamma_i, k_i\} = \gamma_i$. We have to distinguish the cases $w_i = 0$ and $w_i > 0$. The first case implies that $\gamma_i = t_i$ and δ_i included between 0 and t_i, therefore the p_i-part of (α', β') must be of type (x, y) with $\mathrm{o}(x) = p_i^{t_i}$ and this happens in $\frac{p_i^{t_i}}{2p_i^{t_i}-1}$ of the elements of correct order. The second case, i.e. $w_i > 0$, implies $\delta_i = t_i$ and $\gamma_i = t_i - w_i$; this is true in $\frac{\phi(p_i^{t_i - w_i})}{2p_i^{t_i}-1}$ of the possible pairs (ϕ is the Euler's ϕ function).
If $k_i = 0$ then (3.8) becomes

$$\begin{cases} \max\{\gamma_i, \delta_i\} = t_i \\ \delta_i = w_i \end{cases}.$$

Again we have to distinguish two cases depending on w_i. If $w_i = t_i$ then $0 \leq \gamma_i \leq t_i$, this is the same situation of above and happens in $\frac{p_i^{t_i}}{2p_i^{t_i}-1}$ of the elements of correct order. If $w_i < t_i$ then we must have $\gamma_i = t_i$, therefore we get $\frac{\phi(p_i^{w_i})}{2p_i^{t_i}-1}$ of the pairs of correct order.
Finally it remains to analyze the 2-part of (α', β') which is slightly different from the others because $(p-1, p+1) = 2$ (if $p \neq 2$); observe that $k_0 > 0$. If $t_0 = 0$ there is nothing to say since the only solution is $\gamma_0 = \delta_0 = 0$. If $t_0 > 0$ we must distinguish the cases $2 \mid a$ and $2 \nmid a$.

The second case is the easiest: if $2 \nmid a$ then $2 \nmid a'$, which implies $\gamma_0 = 0$ and necessarily $\delta_0 = t_0 = w_0$; this happens in $\frac{1}{2^{t_0+1}-1}$ of the elements of correct order.
We now have to analyze the case $2 \mid a$ which implies $\gamma_0 \geq 1$.
Suppose $k_0 = 1$, then the second condition leads directly to $\delta_0 = w_0$ and, $1 \leq \gamma_0 \leq t_0$ if $w_0 = t_0$ and $\gamma_0 = t_0$ if $w_0 < t_0$. Thus $\frac{2^{t_0}-1}{2^{t_0+1}-1}$ of the elements of correct order in the first case, and $\frac{\phi(2^{w_0})}{2^{t_0+1}-1}$ in the second one.
If $k_0 > 1$, we have $t_0 \leq k_0 + 1$: in particular if $t_0 < k_0 + 1$ then we have $\gamma_0 = t_0$ and $0 \leq \delta_0 \leq t_0 - 1$ and thus $\frac{2^{t_0-1}}{2^{t_0+1}-1}$ of the elements of correct order if $w_0 = 0$; $\delta_0 = t_0$ and $\gamma_0 = t_0 - w_0 + 1$, thus $\frac{\phi(2^{t_0-w_0+1})}{2^{t_0+1}-1}$ of the elements of correct order if $w_0 > 0$.
Finally if $t_0 = k_0 + 1$ then we have to distinguish the cases $w_0 = 0$, $w_0 = 1$, $w_0 = 2$ and $w_0 > 2$. In the first case conditions (3.8) are satisfied if $\gamma_0 = k_0 + 1 = t_0$ and $\delta_0 \leq k_0 - 1$, thus in $\frac{2^{k_0-1}}{2^{t_0+1}-1}$ of the possible pairs; in the second case we must have again $\gamma_0 = k_0 + 1$ while $\delta_0 = k_0$ so $\frac{\phi(2^{k_0})}{2^{t_0+1}-1}$ of the possible pairs; in the third case, i.e. $w_0 = 2$, one easily finds $\delta_0 = k_0 + 1$ and $k_0 \leq \gamma_0 \leq k_0 + 1$ so $\frac{3 \cdot 2^{k_0-1}}{2^{t_0+1}-1}$ of the good pairs; finally if $w_0 > 2$ we obtain $\delta_0 = k_0 + 1$ and $\gamma_0 = k_0 + 2 - w_0$, therefore $\frac{\phi(2^{k_0+2-w_0})}{2^{t_0+1}-1}$ of the elements of correct order.
Summarizing all these informations we get the claim (c). □

This chapter, besides to classify a very special kind of p-adic extensions, shows how difficult can be to obtain an analogous result for extensions of degree p^k with k any natural number using representation theory, even in the simplified case of extensions with no intermediate fields. On the other hand, at present it seems quite hard to find another way that leads to a general solution of the problem of classifying the extensions of degree p^k, therefore it remains to make do of partial results like those showed in the presented work.

Bibliography

[CDC15] L. Capuano and I. Del Corso. A note on upper ramification jumps in Abelian extensions of exponent p. *Rivista di Matematica della Università di Parma*, 6:317–329, 2015.

[Dal12] C.S. Dalawat. Serre's "formule de masse" in prime degree. *Monatshefte für Mathematik*, 166:73–92, 2012.

[DCD07] I. Del Corso and R. Dvornicich. The compositum of wild extensions of local fields of prime degree. *Monatshefte für Mathematik*, 150:271–288, 2007.

[DCDM] I. Del Corso, R. Dvornicich, and M. Monge. On wild extensions of a p-adic field. Submitted.

[FV02] I.B. Fesenko and S.V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, second edition, 2002.

[HK04] X.D. Hou and K. Keating. Enumeration of isomorphism classes of extensions of p-adic fields. *Journal of Number Theory*, 104:14–61, 2004.

[HK06] X.D. Hou and K. Keating. Corrigendum to "Enumeration of isomorphism classes of extensions of p-adic fields". *Journal of Number Theory*, 119:315–316, 2006.

[Iwa55] K. Iwasawa. On Galois Groups of Local Fields. *Transactions of the American Mathematical Society*, 80:448–469, 1955.

[Kra66] M. Krasner. Nombres des extensions d'un degré donné d'un corps p-adic. In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 143–169, Paris, 1966. Editions du Centre national de la Recherche Scientifique.

[Lan94] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Mon11] M. Monge. Determination of the number of isomorphism classes of extensions of a p-adic field. *Journal of Number Theory*, 131:1429–1434, 2011.

[Neu99] J. Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999. Traslation of Algebraische zahlentheorie by Schappacher N.

[PR01] S. Pauli and X.F. Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp.*, 70:1641–1659, 2001.

[Ser77] J.P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977. Traslation of Représentations linéaires des groupes finis by Scott L. L.

[Ser78] J.P. Serre. Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local. *C. R. Acad. Sci. Paris Sér. A-B*, 286:A1031–A1036, 1978.

[Ser79] J.P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.